

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-338826**

(43) Date of publication of application : **10.12.1999**

(51)Int.CI.

G06F 15/00

G06K 17/00

G06K 19/10

H04L 9/32

(21)Application number : 10-139563

(71)Applicant : **HOKURA YUTAKA**

(22)Date of filing : 21.05.1998

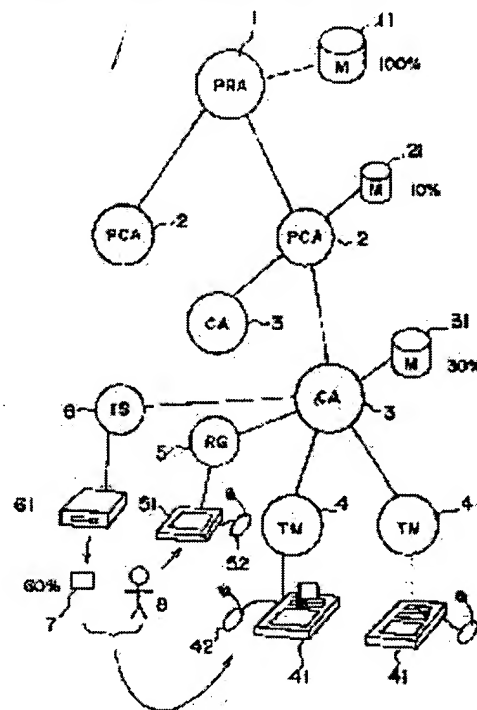
(72)Inventor : **HOKURA YUTAKA**

(54) USER AUTHENTICATION SYSTEM AND USER AUTHENTICATION DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a user authentication system high in security and capable of obtaining the result speedily and to provide a user certificate and a user authentication device to be used for the system.

SOLUTION: Biological feature data such as choreography or voiceprint for distinguishing the individual of a user 8 are acquired, a user certificate 7 recording at least one part of these biological feature data is issued and by comparing the recorded contents of the user certificate 7 read by a certificate reader 41 with the biological feature data of the user inputted to a certification acquiring device, the user is directly certified at a certification utilizing spot 4. Besides, high-order certification stations 2 and 3 are provided, all the biological information of the user is not recorded on the user certificate 7 but the remaining part is recorded for each certification station and by additionally performing the certification while comparing the parts of the recorded biological feature data in response to the reference at the authentication utilization spot 4, the reliability of authentication can be improved.



LEGAL STATUS

[Date of request for examination]

21.05.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3112076

[Date of registration]

22.09.2000

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The registration place equipped with the information incorporation equipment which acquires the biological description data which distinguish a user's individual, The authentication vote publishing office which publishes the user authentication vote which recorded a part of the biological description data [at least] to this user, It is the user authentication system which comes to have the authentication use place in which the **** acquisition equipment which inputs the authentication vote reader and a user's biological description data which read the information on this user authentication vote was formed. By comparing said user's biological description data inputted into the contents of record of a user authentication vote and the aforementioned people certificate acquisition equipment which are read with said authentication vote reader in this authentication use place The user authentication system characterized by attesting that this user is the just owner of this user authentication vote.

[Claim 2] The registration place equipped with the information incorporation equipment which acquires the biological description data which distinguish a user's individual, The authentication vote publishing office which publishes the user authentication vote which recorded a part of the biological description data [at least] to this user, It is the user authentication system which comes to have the authentication use place in which the **** information write-in equipment which inputs the **** acquisition equipment which acquires a user's biological description data, and the this acquired biological description data into said user authentication vote was formed. By comparing said user's biological description data acquired with the contents of the biological description data and the aforementioned people certificate acquisition equipment which were recorded on said user authentication vote using the calculation function of said user authentication vote The user authentication system characterized by attesting that this user is the just owner of this user authentication vote.

[Claim 3] Said user authentication system is equipped with at least one certificate authority further connected by said authentication use place and information channel. The part which is not recorded on said user authentication vote among a user's biological description data acquired in said registration place is recorded on this certificate authority. The user authentication system according to claim 1 or 2 characterized by comparing the part of the biological description data which run short in said user authentication vote in response to the enquiry from said authentication use place, and making it attest.

[Claim 4] The information passed to said information channel is a user authentication system according to claim 3 characterized by enciphering.

[Claim 5] The user authentication system according to claim 3 or 4 characterized by said two or more certificate authorities dividing and recording the part which is not recorded on said user authentication vote among a user's biological description data acquired in said registration place, comparing the part of the biological description data which self memorizes in response to the enquiry from said authentication use place or other certificate authorities for every certificate authority, and making it attest.

[Claim 6] The user authentication system according to claim 1 to 5 characterized by having the certificate authority which formed the storage which records a user's biological description data which said user authentication system acquired in said registration place.

[Claim 7] The user authentication system according to claim 6 characterized by the ability of the storage which recorded the biological description data in said certificate authority to separate from the information channel of this user authentication system.

[Claim 8] A user authentication system given in either of claims 1-7 characterized by said biological description data being a hand.

[Claim 9] A user authentication system given in either of claims 1-8 characterized by conducting the dealings which register two or more things as said biological description data, and change with inputted data.

[Claim 10] The user authentication vote which consists of a storage equipped with the storage region which recorded some biological description data [at least] which are the user authentication vote which can be used for a user authentication system given in either of claims 1-9, and distinguish the individual of the signal and user who identify an identification tag, and in which read-out is possible.

[Claim 11] The user authentication vote according to claim 10 characterized by furthermore having CPU and RAM.

[Claim 12] The user authentication vote according to claim 10 or 11 characterized by said storage being a magnetic-recording medium.

[Claim 13] The user authentication vote according to claim 10 or 11 characterized by said storage being an IC card.

[Claim 14] User-authentication equipment equipped with the judgment equipment which compares said user's biological description data inputted into the authentication vote reader which reads the information recorded on a user-authentication vote, the **** acquisition equipment which input a user's biological description data, and the biological description data and the aforementioned people certificate acquisition equipment which are recorded on the user-authentication vote which read with said authentication vote reader, and judges success or failure, and the display which output a judgment result.

[Claim 15] User authentication equipment according to claim 14 characterized by the aforementioned people certificate acquisition equipment being what has a freehand drawing form incorporation function.

[Claim 16] Furthermore, user authentication equipment according to claim 15 or 16 characterized by having the communication device which transmits some a user's biological description data [at least] inputted into **** acquisition equipment to an external certificate authority, and receives the judgment result of success or failure, and displaying a judgment result through said display.

[Translation done.]

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the user authentication system for performing personal authentication in electronic information interchange or electronic commerce, the user authentication vote used for this, and user authentication equipment.

[0002]

[Description of the Prior Art] In recent years, the class of information accessed through a communication network is becoming Oshi extremely, and as well as electronic commerce, such as dealing of goods and a credit, perusal of the registration matter in the online diagnostics in medicine, an individual clinical recording, and a public office, issue of certification, etc. also increase an object increasingly, and it is in the inclination for use to progress.

[0003] When there is no guarantee of not revealing to others with respect to privacy in such individual information, there are not few things which should accept use and it is supposed that are not come out. In order to incorporate development of an electronic intelligence communication network and to build a more convenient information society, the user authentication method with the high dependability which can distinguish an individual sharply is called for. Moreover, the device which attests an individual correctly is applicable also to the locking equipment which restricts ingress other than the rating person in a lab, a place of business, or a residence, and the improvement in security of cybermoney.

[0004] Conventionally, the password has been best used for user authentication. Although the password is simple, those who use others' password by stealth and become him completely cannot be eliminated. For this reason, the suitable cautions of choosing the password which is hard to guess, sometimes changing a password, etc. which use a long password tend to be carried out, and it is going to secure safety. Moreover, it is also performed widely that others take care not to know the contents easily even if it makes the contents of a communication link secret using encoding technology and there is leakage of data, in order to secure the safety in a communication link process.

[0005] however -- still -- communicative tapping and decode of a cipher -- stealing -- seeing -- etc. -- a password may be stolen and it cannot change with a completely safe thing. Moreover, there is a fault to which it becomes difficult for the user itself to memorize it correctly, so that a password is complicated. Even if it is data complicated still more essential however, there is a property to become possible to reproduce with a certain means from the moment that it is stored as digital data.

[0006] In order to prevent spoofing and to attest certainly that he is him, how to carry out user authentication using the information showing the so-called biological descriptions, such as a fingerprint and a voiceprint, is also examined. However, generally, since the biological description data have large amount of information, huge traffic must be exchanged between the use site which needs authentication, and the certificate authority which is accumulating a user's living thing-information. Therefore, it is difficult to put in practical use except in the case in a special environment because of the congestion of a channel, or huge-izing of communication link time amount, and the problem was in the management location and management method of the data.

[0007]

[Problem(s) to be Solved by the Invention] Then, the technical problem which this invention tends to solve is that the safety for performing personal authentication in electronic information interchange or electronic commerce offers the user authentication vote and user authentication equipment with which it is used for this with the user authentication system from which a result is obtained quickly highly.

[0008]

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, the user authentication system of this invention The registration place equipped with the information incorporation equipment which acquires the biological description data which distinguish a user's individual, The authentication vote publishing office which publishes the user authentication vote which recorded a part of the biological description data [at least] to the user, It has the authentication use place in which the authentication vote reader which reads the information on a user authentication vote, and the **** acquisition equipment which acquires a user's biological description data were formed. It is characterized by carrying out user authentication by comparing a user's biological description data acquired with the contents of record and **** acquisition equipment of the user authentication vote read with the authentication vote reader of an authentication use place.

[0009] Moreover, the 2nd user authentication system of this invention The registration place equipped with the information incorporation equipment which acquires a user's biological description data, The authentication vote publishing office which publishes the user authentication vote which recorded a part of the biological description data [at least] to the user, It has the authentication use place in which the **** information write-in equipment which inputs the **** acquisition equipment which acquires a user's biological description data, and the acquired biological description data into a user authentication vote was formed. It is characterized by attesting that he is the just owner of a user authentication vote by comparing a user's biological description data acquired with the contents and **** acquisition equipment of the biological description data currently recorded using the arithmetic unit of a user authentication vote.

[0010] The user authentication system of these this inventions is further equipped with at least one certificate authority connected by the authentication use place and the information channel. Except for some a user's biological description data acquired in the registration place, it records on the user authentication vote. It is desirable to record the part which is not recorded on a user authentication vote on the certificate authority, to compare the part of the biological description data which run short in a user authentication vote in response to the enquiry from an authentication use place, and to make it attest. In addition, as for the information mutually exchanged through an information channel, it is desirable to encipher and to guarantee safety.

[0011] Moreover, it is more desirable for there to be two or more certificate authorities, to divide and record the part which is not recorded on a user authentication vote among a user's biological description data acquired in the registration place, to compare the part of the biological description data which self memorizes in response to the enquiry from an authentication use place or other certificate authorities for every certificate authority, and to make it attest. Furthermore, a user authentication system may be equipped with the certificate authority which formed the storage which records a user's biological description data acquired in the registration place. Moreover, as for the storage which recorded the biological description data in a certificate authority, it is desirable that it can separate now from the information channel of a user authentication system. In addition, a hand may be used as biological description data.

[0012] The user authentication system of this invention uses the user authentication vote which recorded some biological description data [at least] which distinguish a user's individual, and since user authentication is carried out by comparing the biological description data and the biological description data of a user authentication vote which the user inputted and it cannot pass an authentication test if it is not the user itself, it can prevent spoofing by theft of a password.

[0013] Moreover, being very difficult and since others cannot reproduce the biological description even if restoration is possible, restoring the original biological description data from the digital-data-ized

biological description data has the very high dependability of user authentication. Since the biological description data for enquiry are especially recorded on the user authentication vote, even if I do not have user authentication carried out by the remote certificate authority, in the authentication use place which needs authentication, it can check directly that he is him. For this reason, it is not necessary to spend great time amount and costs on the communication link with a certificate authority.

[0014] In addition, although user authentication can also perform contrast with the biological description data of the user who made it input in the biological description data and the authentication use place for the enquiry recorded on the user authentication vote with the arithmetic and logic unit formed in the authentication use place. It has calculation functions, such as CPU and RAM, in a user authentication vote, and you may make it contrast with the information which inputs the biological description data acquired from the user who is going to use a user authentication vote, and is recorded. The burden of an authentication use place shall be mitigated, equipment cost shall be reduced, and it shall be easy to use as a system by utilizing the user authentication vote which has advanced functions, such as an IC card. Moreover, by completing information processing within a user authentication vote in this way, it can prevent revealing authentication data to the exterior of an authentication vote, and safety can be raised.

[0015] Furthermore, the remaining part which is not recorded on a user authentication vote among a user's biological description data is recorded on the certificate authority connected by the authentication use place and the information channel. When comparing the part of the biological description data in response to the enquiry from an authentication use place and making it attest. Since required information is divided and memorized, even if it restores the biological description data from the data recorded, for example on the authentication vote, it cannot break through an authentication system, and the data used for authentication from an authentication vote cannot be reproduced, either. Moreover, since the information in a certificate authority is preserved even if it alters the contents of storage of an authentication vote, others' spoofing can be eliminated. Or since it cannot alter again to the information on the user authentication vote which a user owns also when a certificate authority is attacked, it is safe. In addition, if the information passed to an information channel is enciphered, since it is hard to decode even if there are those who steal information in the middle of a channel, safety will improve.

[0016] Moreover, a user's biological description data are divided and recorded by the user authentication vote and two or more certificate authorities. To the user authentication based on the information on a user authentication vote, in addition, when the part of the biological description data memorized in response to the enquiry from an authentication use place or other certificate authorities for every certificate authority is compared and it is made to attest. For example, dependability of user authentication can be made higher by acquiring gradually the user authentication of the certificate authority organized hierarchical.

[0017] In addition, in the user authentication system of this invention, even if it chooses making a success-or-failure decision according to the grade of the authentication dependability demanded by the authentication of only an authentication use place based on the information recorded on the user authentication vote, the authentication in one piece or two or more certificate authorities which seasoned the user authentication vote with the information which is not recorded may be added, and a more positive judgment may be chosen. For example, to not performing user authentication so carefully [when trading in the goods of a small amount], to treat large sum goods, a more advanced guarantee is required, and to treat the thing concerning advanced privacy like the clinical recording of a hospital, it is necessary to check whether it is his claim certainly.

[0018] The level to the safety of such authentication may be beforehand decided an authentication use place and for dealings, and may be set up for every dealings in an authentication use place. Furthermore, in connection with a dealings price etc., it chooses automatically, and you may enable it to set up. Moreover, even when performing user authentication using all of the biological description data even if, in order that most may attest in an authentication use place using the information in a user authentication vote according to this information-sharing method, since the amount of information exchanged through a communication circuit is an element, its communication circuit capacity may also be small and there is also little time amount which enquiry takes again. In addition, dividing information has the effectiveness

which controls the demand of the throughput in the certificate authority which accumulates information about many users and must process much enquiry, or storage capacity.

[0019] Furthermore, it has the qualification registration authority which formed the storage which records a user's biological description data acquired in the registration place on a user authentication system. It can use for repair of the data of a recurrence line when the judgment of the location where a certain unauthorized use and abnormalities occurred, or an authentication vote is damaged, and a low-ranking certificate authority etc. by recording the whole picture of a user's biological description data acquired in the registration place.

[0020] Moreover, if it is made for the storage which recorded the biological description data in a qualification registration authority to use it, connecting [enabling it to separate from the information channel of a user authentication system, and] only when required, it can prevent individual humanity news being revealed by a hacker's invasion etc., or being altered. In addition, it is very effective in order for recording only the respectively partial biological description data on the certificate authority of a user authentication vote or low order, and making it not leave perfect record to secure safety.

[0021] A hand may be used as biological description data used by the user authentication system of this invention. A hand expresses the individual biological description well, and others' spoofing is difficult for it, and it has the advantage that the equipment to input and which is equipment [equipment] and analyzed is obtained comparatively easily. In order to identify a user, it is easy to be suitable [the alphabetic character or graphic form which are written and got], but since the sign showing a self name etc. has good repeatability, it cannot be overemphasized that it is desirable. Moreover, in addition to this, there are a pattern of a fingerprint, palm print and a voiceprint, the iris, or a retina, DNA information, etc. in the available biological description data. The biological description which can be recognized more certainly and easily may be found out from now on also.

[0022] In addition, when dividing and recording the biological description data by the user authentication vote and the certificate authority Information data are divided physically and a part for the first portion is recorded on a user authentication vote, and a part is recorded on a certificate authority and you may make it collate it in the second half. Moreover, methods of catching information hierarchical and dividing it, such as recording the configuration information on a hand on a user authentication vote, for example, and recording writing pressure information and order-of-making-strokes-in-writing-a-Chinese-character information on a certificate authority, may be used. Furthermore, it is also possible to raise dependability by judging two or more biological description data, such as a sign and a voiceprint, based on the information on a class which records separately and is different, respectively.

[0023] In addition, you may constitute so that the dealings which register two or more things as biological description data, and change with inputted data may be conducted. If the information which gave special implications is compounded besides the biological description data of normal, and it is made to use, and it will hide in somewhere in signs and a notation will be added when it lapses into the situation which is threatened by others and cannot but sign against volition, for example, it can also be made the structure of pretending to sign the extortion person obediently and notifying a security company in fact.

[0024] In addition, as selection of system style Chikujo, since the insurance on a human body is secured in such a case, things made to look like dealings being materialized ordinarily, such as closing motion of a door and a drawer of cash, are also possible. Of course, the biological description data used for such a purpose may be the thing of the same class as a formal thing, and may compound the thing of a class which is [add /, for example to a sign / voice data] different. Moreover, it is good conversely also considering what added specific agreement data to false data as formal data for authentication.

[0025] In addition, in order to solve the above-mentioned technical problem, the user authentication vote of this invention is characterized by consisting of a storage equipped with the storage region which recorded some biological description data [at least] which distinguish the individual of the signal and user who identify an identification tag and in which read-out is possible. Although the record medium only for [, such as ROM and CD-ROM,] reading may be used, since the contents of record are the

information showing a user's biological description and there is little risk of an alteration as a storage, it is possible for it to be also the storage in which write-in reading which can add and record the contents of dealings and new information is possible.

[0026] It is desirable to have a high forged prevention function and big data volume, and to use especially, an IC card with high intelligent function and security function which carried the code system. Moreover, when using the IC card which carried CPU and RAM, the biological description data acquired from the user are incorporated in a card, if it is made to perform user authentication as compared with the data for enquiry memorized inside, the burden of an authentication use place can be mitigated and equipment cost can be reduced. Moreover, safety can be raised as the authentication data of a user authentication vote cannot be read from the exterior.

[0027] in addition, the thing for which an IC card is used -- a complex function -- carrying -- advanced him -- it can be made the multiple use card which has an authentication function. The IC card used here may be a compound IC card which compounded the non-contact type which does not depend on the contact process and external terminal which are written with an external terminal, but is written by non-contact. Since especially the user authentication vote of this invention is not helpful even if it alters the contents of record when distributing and using information, it may use a more economical and simple floppy disk. Moreover, in addition to this, various kinds of record media which can be written in, such as CD-ROM, DVD, a tape, and MD, can be used.

[0028] In order to solve the above-mentioned technical problem, moreover, the user authentication equipment of this invention The authentication vote reader which reads the information recorded on the user authentication vote, and the **** acquisition equipment which acquires a user's biological description data, It is characterized by having the judgment equipment which collates the biological description data currently recorded on the user authentication vote read with the authentication vote reader, and a user's biological description data acquired with **** acquisition equipment, and judges success or failure, and the display which outputs a judgment result.

[0029] While applying a user authentication vote to an authentication vote reader according to the user authentication equipment of this invention If the user who was able to search for authentication inputs the biological description data of the same class as what was recorded on the user authentication vote through **** acquisition equipment Since the result of having collated the biological description data with which judgment equipment was recorded on the user authentication vote, and the biological description data acquired with **** acquisition equipment, and having judged success or failure is displayed on a display, even if it does not communicate with the exterior, it can recognize immediately whether you are a Shinsei user authentication vote owner.

[0030] In addition, it is necessary to equip user authentication equipment with the **** acquisition equipment of the same class as the biological description data entry unit installed in a user registration place. What has a freehand drawing form incorporation function as **** acquisition equipment can be used. If the freehand drawing form of arbitration decided beforehand, such as a sign, is inputted as digital data using a freehand drawing form incorporation function, it will become possible easily to compare with the biological description data of a user authentication vote.

[0031] Furthermore, as for the user authentication equipment of this invention, it is desirable to have the communication device which can communicate with an external certificate authority, to transmit some a user's biological description data [at least] inputted into **** acquisition equipment to an external certificate authority, and to display a judgment result for the judgment result of success or failure through reception and a display. By connecting with an external certificate authority and treating authentication data hierarchical, access and an alteration of a trespasser with malice are prevented and it becomes possible to have the high authentication capacity of safety more.

[0032]

[Embodiment of the Invention] Hereafter, with reference to a drawing, the detail of this invention is explained based on an example. The block diagram showing the example of the user-authentication vote which uses the block diagram in which drawing 1 shows one example of the user authentication system of this invention, the perspective view showing the example of the user authentication equipment which

uses drawing 2 for this example, and drawing 3 for the block diagram of user authentication equipment, and uses drawing 4 for this example, the flow chart showing the example of a procedure for which drawing 5 publishes the user-authentication vote in this example, and drawing 6 are the flow charts showing the example of a procedure of the authentication in a use place.

[0033]

[Example 1] The user authentication system of this example has the layered structure which consists of a qualification registration authority, a certificate authority, and an authentication use place, as shown in drawing 1. qualification -- a registration authority (PRA) -- one -- authentication -- a network -- the whole -- generalizing -- a thing -- it is -- a licensee -- ***** -- plurality -- middle -- a certificate authority (PCA) -- two -- a part -- authority -- giving -- a certificate -- publishing -- authority -- giving -- having had -- middle -- a certificate authority -- a sublicensee -- ***** -- plurality -- an end -- a certificate authority -- (-- CA --) -- three -- a part -- authority -- giving -- a certificate -- publishing .

[0034] an end -- a certificate authority -- (-- CA --) -- three -- user authentication -- using -- a client -- becoming -- authentication -- use -- a place -- (-- TM --) -- four -- a client -- service -- it is going to use -- a user -- eight -- interceding -- an engine -- becoming . In addition, in the following explanation, use of various services may be expressed as dealings. In addition, the qualification registration authority (PRA) 1 had the storage 11 separable from equipment, and the middle certificate authority (PCA) 2 and the end certificate authority (CA) 3 are equipped with the storage 21 and 31 always connected to equipment.

[0035] These engines are connected by the dedicated line or the public line, respectively, and it has come to be able to perform informational exchange at any time. In addition, it is good also by connection using an intranet network or the Internet network. When exchanging information using these communication lines, it is desirable to secure insurance by performing encryption processing which used the public key and the common key. In addition, a middle certificate authority (PCA) is omissible when building a user authentication system. Moreover, in preparation for multistage, a hierarchy's depth may be larger than three steps about the middle certificate authority (PCA). In addition, it cannot be overemphasized that the engine which coalesced mutually may be made to perform functions, such as a qualification registration authority (PRA), a middle certificate authority (PCA), and an end certificate authority (CA).

[0036] Generally the authority about fields which restricted the object, such as an administrative body, a medical institution, a specific company, an apartment house, and a shopping center (mall), is awarded to the end certificate authority (CA) from the qualification registration authority (PRA) or the certificate authority (PCA) of a high order. an end -- a certificate authority -- (-- CA --) -- three -- **** -- this -- authority -- having -- a field -- belonging -- user authentication -- using -- authentication -- use -- a place -- (-- TM --) -- four -- connecting -- having -- **** .

[0037] Various kinds of things [, such as a pay counter of a large-scale retailer and a bank / such as a window an automated-teller etc. of financial institution,], such as each store, a department store, etc. of the door of the information machines and equipment which access the door of each window of a public office, subject reception of a hospital and chemist's shop reception, a lab, or a department-and-section room and the database which needs protection, an apartment inlet port, or a single room, the remote control of an indoor utility, the facility of membership system crab, and a mall, are one of the things applicable to the authentication use place (TM) 4. The user authentication especially in direct marketing serves as a future still more important technical problem, and the situation of installing the authentication use place 4 in each user's 8 house is also considered.

[0038] The end certificate authority (CA) 3 grants the authority to grant the authority to receive registration for the user 8 who is going to use the authentication use place (TM) 4 to the user registration place (RG) 5, and to publish the user authentication vote 7 in the authentication vote publishing office (IS) 6.

[0039] The user registration place (RG) 5 is equipped with the input unit 51 which acquires the biological description. In this example, the online freehand drawing form input unit which consists of a tablet and a pen is used. If a hand is inputted from an online freehand drawing form input unit, since the information on a writing process can be incorporated together and can carry out image measuring, also

when an alphabetic character is inputted, for example, the information on the ability of each **** to have started [in what kind of direction] in which sequence etc. can be acquired easily.

[0040] Moreover, when using a voiceprint as a means to catch the biological description, a microphone 52 is equipped and voice is inputted. In addition, you may have the equipment which incorporates a fingerprint and palm print, and equipment which observes a pupil and incorporates the iris and a retina pattern. By using together two or more these people certificate means, **** can also be made more reliable.

[0041] Authentication vote issue equipment 61 is installed in the authentication vote publishing office (IS) 6. Authentication vote issue equipment 61 writes in the information used for the user authentication vote 7 at ****, and grants it to a user 8. Although the IC card constituted the user authentication vote from the user authentication system in this example, other electronic recording media, such as magnetic-recording media, such as CD-ROM, a floppy disk, and a magnetic card, or a magneto-optic-recording medium, can also be used that what is necessary is just the record medium in which write-in read-out is possible.

[0042] The user authentication equipment 41 which inspects Shinsei of the user authentication vote 7 which the user 8 has, and attests a user 8 is formed in the authentication use place (TM) 4. Drawing 2 and drawing 3 are drawings in which the example of 1 configuration of user authentication equipment 41 is shown. I/O device 401 which exchanges the storage region and the information on the authentication vote 7 by which the slot which inserts the authentication vote 7 was inserted in the top face of user-authentication equipment 41 by being, the authentication level assignment equipment 402 which specifies the depth of the authentication required of dealings, the **** input unit 403 which acquire a user's biological description data, and the authentication display 404 which display an authentication result are arranged.

[0043] In addition, the **** input unit 403 is the same as the biological description input unit 51 used in the user registration place (RG) 5. Therefore, when using a voiceprint together to user authentication, it cannot be overemphasized that it is necessary to attach a microphone 42 also to the user authentication equipment 41 of the authentication use place (TM) 4. Thus, the **** input device 403 is equipped with the input device which suits in order to acquire it according to the class of biological information data of the user who uses.

[0044] Moreover, the electronic circuitry 410 which combines these equipments organically and performs user authentication is built in the interior of user authentication equipment 41. This electronic circuitry 410 consists of the authentication vote read write control unit 411, **** signal transduction equipment 412, judgment equipment 413, and a communication device 414. The authentication vote read write control unit 411 is equipped with the function to decrypt the digital data which read the contents of record of an authentication vote and was enciphered through I/O device 401, and to make an authentication vote memorize a dealings result again.

[0045] Moreover, **** signal transduction equipment 412 changes into digital data the biological description data incorporated with the **** input device 403. Judgment equipment 413 considers the information which incorporated the print-out of the authentication vote read write control device 411, **** signal transduction equipment 412, and authentication level assignment equipment 402, and exchanged it with the certificate authority through the communication device 414 according to the authentication level needed, performs a user's personal authentication, and displays a result on the authentication display 404.

[0046] Since a dealings result will be inputted from the contents input unit 420 of dealings and the contents will be displayed on the dealings display 421 if user authentication is performed and dealings are materialized, a user 8 can also check this. Moreover, the contents of dealings are recorded on storage 422. In addition, a user authentication result may be made to be made to the contents input unit 420 of dealings by judgment equipment 413 as for acceptance or refusal of delivery and dealings automatically.

[0047] Furthermore, dealings information is inputted from the contents input unit 420 of dealings, and you may make it record the contents of dealings, and dealings hysteresis on the user authentication vote

7. For example, it will pay, if the trade date, the purchase trade name, and the price are recorded when using the user authentication vote 7 for the settlement-of-accounts field, and the contrast check at the time becomes easy. Moreover, by the authentication vote for administration service, certification documents, such as a health insurance card, a driver's license, medical information, or a basic resident register, are received in the user authentication vote 7, and can be saved. moreover, the thing been contingent [on user authentication] when perusing the contents recorded on the user authentication vote 7 -- him -- access of an except can be eliminated and individual privacy can be protected.

[0048] In addition, the information which gave special implications is compounded besides the biological description data for using for right authentication, and you may make it use. For example, although dealings will be ordinarily materialized by closing motion of a door, the drawer of cash, etc. if a hidden notation is casually added to the sign of normal when it lapses into the situation which is threatened by a burglar, the blackmailer, etc. and cannot but sign against volition It seems that the structure which performs suitable treatment, such as the report having gone for coincidence also to the security company, and arresting a criminal in the place which changed into the condition that a user's insurance was secured, can be given. Giving a cough twice lightly etc. may compound and use the thing of a different class at the same time it considers as the biological description data used for such a purpose, for example, signs.

[0049] Drawing 4 is the block diagram showing the internal configuration of the user authentication vote which used the IC card. The user authentication vote 7 used by this example takes into consideration facilities for two or more publishers to install a shared terminal, and do mutual release together.

Although the compound-die IC card equipped with both non-contact molds which communicate by the electrostatic coupling, electromagnetic induction, etc. without the contact mold which transmits an electrical signal through the connection terminal 71, the electrode 73 in a card, and the electrode in an authentication vote read write control unit contacting is adopted One of methods may be furnished.

[0050] The communications control circuit 74 is connected to the connection circuit 72 and the non-contact electrode 73, and it connects with the memory to build in at the connection terminal 71. The user authentication vote 7 is equipped with the memory and CPU75 which serve as electrically random access memory RAM 76 and read-only memory ROM77 from eliminable programmable read-only memory EEPROM79 with programmable read-only memory PROM78 which can be written in, and mutual is connected by the bus. The connection circuit 72, the communications control circuit 74, CPU75, and memory can be held in one IC chip.

[0051] The authentication vote read write control unit 411 can access the memory of the user authentication vote 7 through the non-contact electrode 73 to the communications control circuit 74 through the connection circuit 72 from the connection terminal 71, if the user authentication vote 7 is inserted. The data which ID to clarify was stored and once wrote in the publisher who published the user authentication vote in response to card authentication data and certification which are used in order to inspect the bona fides of an authentication vote to PROM78 cannot be rewritten. Record of the dealings using the biological description data used for a user's authentication or an authentication vote is stored in EEPROM79. Moreover, CPU75 is controlled to ROM77 and the program which conducts control of encryption, a decryption, and data I/O, bona-fides inspection of user authentication equipment 41, etc. is stored. RAM76 has the function to hold the data incorporated from the outside, and the data which are needed in an operation process temporarily.

[0052] The user authentication vote 7 is distributed to each authentication vote publishing office 6, where the right card qualification information which it can guarantee that it is the proper card used for a system in the qualification registration authority 1 is written in PROM78. Therefore, the authentication vote publishing office 6 should just write some a user's biological description data in EEPROM79 based on the directions from the qualification registration authority 1. In order to make it not accept the alteration of a card, you may make it authentication vote issue equipment not equipped with the rewriting function of PROM78. However, memory allocation of the authentication vote in this example may record the biological description data for not being restricted above, for example, performing he authentication on PROM78 or RAM76.

[0053] One example of a procedure which publishes a user authentication vote using drawing 5 is explained. A registration application is received from the user 8 who wants the user registration place 5 to receive service of the authentication use place 4 in the jurisdiction field (S11). At this time, the user registration place 5 acquires the information showing a user individual's biological description while hearing the information used for a user's 8 prequalification if needed (S12). What has the property which can be detected even if the biological description used here is peculiar to a user individual, and others are going to become the user by imitation, disguise, etc. and clear up is chosen.

[0054] He is trying to identify in this example using a hand. Although the graphic form to input may be arbitrary, since differing whenever a user 8 inputs is out of order when attesting, in order to guarantee repeatability, it is usually desirable to make the sign showing a self name input. In addition, since the safety of authentication will improve if two or more biological descriptions are used, it enables it to also acquire the voiceprint using the microphone 42 auxiliary. A proposer's rating information and biological description data which were extracted in the user registration place 5 are transmitted to the qualification registration authority 1 (S13).

[0055] The qualification registration authority 1 screens based on the information received from the user registration place 5, and permits issue of an authentication vote to those who passed (S14). Since qualifying requirements are decided according to the object using authentication, you may make it examine by the end certificate authority 3 which actually accepts a user. The qualification registration authority 1 divides a registered user's 8 biological description data hierarchical according to a predetermined rate, determines the part distributed to the certificate authorities 2 and 3 of the user authentication vote 7 and each phase, and distributes to every place (S15).

[0056] The biological description data distributed to every place in the qualification registration authority 1 It is what is accessed based on the authentication precision which the authentication use place 4 requires. It enables it to attest only by the result contrasted with the authentication equipment 41 of the authentication use place 4 when the dependability of most low degree was sufficient. When requiring the dependability of whenever [inside], considering and carrying out user authentication of the information stored in the end certificate authority 3 and requiring the most advanced guarantee, all the biological description data by which distributed storing was carried out are unified, and it is made to judge.

[0057] Only when bona fides are inspected and it passes first in the authentication use place 4, the biological description data consist of user authentication systems of this invention so that a high order engine's authentication can be charged. In the certificate authority of a high order, authentication using the information on the part which is not in a user authentication vote is performed. Therefore, the information which can judge that he is the Shinsei user with a certain amount of accuracy must be distributed to the user authentication vote 7 by contrasting with the biological description data which the minimum user 8 inputs.

[0058] In this example, we distributed about 60% of information to the user authentication vote 7, and decided to distribute 10% of remaining information at 30% of information, and the middle certificate authority 2 at the end certificate authority 3. Thus, by decreasing amount of information in series, the effectiveness of decreasing the time amount load which saves the storage capacity of the high order engine for which much authentication claims gather more, and authentication takes arises, and improvement in the information-protection engine performance as the whole system can be aimed at.

[0059] In addition, when a more advanced guarantee is demanded, in order for the information sent to the engine of a high order not to become excessive, the one where the rate of the biological description data held to the user authentication vote 7 is to some extent larger is desirable. However, if the ratio of the information given to the user authentication vote 7 becomes excessive, the dependability of user authentication will fall. Therefore, it is necessary to take into consideration the number of users to connect, the safety of the authentication demanded, etc. in distribution of the biological description data, and to define the suitable division rate which suited actual conditions.

[0060] The informational division approach may be divided as the information about **** in the middle of drawing with the information about the configuration which it finished drawing like a hand, and

information which followed the phase further like information, such as the order of making strokes in writing a Chinese character, although you may be the approach of predetermined coming out of the digital-information-ized data comparatively, and dividing physically. For example, a voiceprint can be divided into a frequency band, or each biological description, such as dividing a fingerprint for every finger, and recording and using for each, can be divided suitably, and can be used. In addition, two or more descriptions, such as a hand and a voiceprint, may be divided and used for every class which acquires and is different.

[0061] When a magnetic tape, CD-ROM and a magneto-optic disk, DVD, or a removable hard disk recorded and saves the information about an authentication vote and a user for the mass storage means 11 separable from equipment (S16) and the qualification registration authority 1 has a request from a low order engine, an official in charge refers for the information equipped with and registered into the regenerative apparatus. In the authentication registration authority 1, since the information record medium 11 is separated from an external communication circuit network at the time of needlessness and is kept using the dismountable recording device 11, the invasion from the outside and an alteration can be prevented.

[0062] the individual biological description data distributed to certificate authorities 2 and 3 are stored in the alike and attached storage 21 and 31, respectively, and if needed, reading appearance of them is carried out at any time, and they are used. The authentication vote publishing office 6 records the biological description data of the registration proposer who received distribution in the user authentication vote 7 on which the card authentication code decided for every authentication vote is recorded from the qualification registration authority 1, and pays them to a user 8 (S17).

[0063] in addition -- one -- a piece -- an end -- a certificate authority -- (-- CA --) -- three -- plurality -- user registration -- a place -- (-- RG --) -- five -- authentication -- a vote -- a publishing office -- (-- IS --) -- six -- you may have . Since it must report to the user registration place 5 and the own biological description must actually be inputted, a user 8 is desirable because of a user's 8 facilities, when the authentication vote publishing office 6 which receives the published user authentication vote 7 is installed in the same location as the user registration place 5.

[0064] In addition, it may be made to be contingent [on the presence of the person who can set reliance for a user's 8 ****]. However, no matter what device it may use, it is difficult to eliminate completely the case where became others from the start and it is clearing up. Moreover, in order to check the fact which the user who registers notified, not the method that publishes an authentication vote to a registration procedure and coincidence but the method mailed to the address behind may be adopted. In addition, the qualification registration authority (PRA) 1 may be made to have the user registration place (RG) 5 and the authentication vote publishing office (IS) 6. furthermore -- user registration -- a place -- (-- RG --) -- five -- authentication -- a vote -- a publishing office -- (-- IS --) -- six -- a function -- having had -- a portable remote terminal -- having had -- a publisher -- arbitration -- a location -- setting -- registration -- issue -- a procedure -- carrying out -- things -- being possible . Only those who received rating qualification of normal from the qualification registration authority (PRA) need to take care not to accept use of such a portable remote terminal, and it is constituted so that it can be begun and operated in response to the severe authentication as a publisher also here.

[0065] Next, one example of the procedure which carries out user authentication by the user authentication vote 7 in the authentication use place 4 is explained using drawing 6 . If a user 8 submits the user authentication vote 7 and offers dealings to the authentication use place 4, the authentication use place 4 will insert the authentication vote 7 in the card slot (I/O device) 401 of authentication equipment 41, and will read the information for authentication. The information for checking the bona fides of a card and the biological description data for user authentication are contained in the information for authentication.

[0066] The authentication use place 4 attests a card first (S21). Authentication of a card is Shinsei the user authentication vote's 7 being adapted for the user authentication system which the authentication use place 4 uses, and checking who a just possessor being. When the not corresponding authentication vote is being used, dealings are not received from the start. In addition, in order to check that the user

authentication vote 7 is not accessed unjustly conversely, it verifies whether authentication equipment 41 is an own authentication vote and a thing by the program in the user authentication vote 7, and when it is not right authentication equipment, you may have the structure which refuses the indication of the contents of storage.

[0067] The thing for which the same biological description as what was used when the user authentication vote 7 was acquired is displayed, such as writing and getting a sign from a user 8 on a tablet (person certificate input unit) 403, when it passes by card authentication, is searched for (S22). And the biological description data inputted from the tablet 403 are collated with 60% of biological description data currently recorded on the user authentication vote 7, and the user 8 of a window judges whether you are the Shinsei possessor of the user authentication vote 7 (S23). A user authentication result is displayed on a display 404 (S24).

[0068] Procedures differ according to the success or failure of the user authentication in the authentication use place 4 (S25). When user authentication is denied, the authentication use place 4 refuses dealings (S33). When user authentication is passed, it investigates whether the certificate authority of a high order should be further asked for online authentication (S26). When you do not need online authentication, you may accept the proposal of dealings immediately (S32). Whenever [existence / of a demand of online authentication / or demand / of the depth] may be made to be set up automatically based on the character of dealings, or the amount of the dealings amount of money, although an operator and a user 8 may input from authentication level assignment equipment 402 for every dealings.

[0069] When you need online authentication, it sends ***** people certificate information to the end certificate authority 3 with the information and the **** input unit 403 of the user authentication vote 7 with the demand of authentication level (S27). Since 40% of part is sufficient, for example, the **** information to send can cut down the amount of information which excepted the part used in the authentication use place 4 and which is exchanged between the authentication use place 4 and the end certificate authority 3.

[0070] The necessity of online authentication is decided by the demand level over the safety of authentication according to the character of dealings. Since authentication safer for dealings of the high goods of liquidity and large sum goods or disclosure of individual confidential information is needed, a high order engine's user authentication will be called for. Moreover, the depth of online authentication may be specified by the character of the authentication use place 4. in order to guarantee protection of privacy, and an exact therapy action at the window of a hospital -- advanced him -- authentication is needed in many cases. In addition, in order to check that it is his data certainly with the home medical examination using a communication line, it is desirable to ask for user authentication to the certificate authority of a high order.

[0071] In the end certificate authority 3, it collates with the **** information on a user's 8 proper currently recorded on storage 31 (S28), and an authentication result is sent to the authentication use place 4 (S29). Since it is recorded on the end certificate authority 3 30% of a user's **** information, when it runs short only by the user authentication in here, the middle certificate authority 2 of a high order is further asked for user authentication. Since 10% of biological description data are recorded on the middle certificate authority 2 about each user, the part used by the middle certificate authority 2 among ***** people certificate information in the authentication use place 4 becomes 10%, and the amount of information which should be sent to the middle certificate authority 2 from the end certificate authority 3 decreases still more sharply. The user authentication result performed by the middle certificate authority 2 returns to the authentication use place 4 through the end certificate authority 3.

[0072] A user authentication result in each place is synthesized in the authentication use place 4, and is displayed on the authentication display 404 of user authentication equipment 41. When user authentication is success, dealings will be accepted (S32), and in a rejected case, dealings will be refused (S31). (S33) Moreover, since there is possibility of some malfeasances, such as an alteration and spoofing, when user authentication is denied, it is desirable to send the information to the qualification registration authority 1, to check the whereabouts in question, and to analyze a cause.

[0073] Since it trespasses upon the qualification registration authority 1 from the outside or record with it difficult [to alter] is kept, it becomes clear by contrasting with the input data in the authentication use place 4 whether it is in that abnormalities are in the user authentication vote 7, or it is in the end certificate authority 3 or the middle certificate authority 2. When a disagreement is between the information which the contents and the user 8 of the user authentication vote 7 inputted, the case where the data of the case where the user who is not Shinsei is using it by the theft or finding, or a user authentication vote are rewritten by unjust access can be considered.

[0074]

[Example 2] The point that the user authentication system of this example differs from the 1st example Instead of carrying out with the logic unit formed in the authentication use place by contrasting the biological description data of the user who made it input with the biological description data recorded on the user authentication vote, and **** acquisition equipment Since it is only the point of having contrasted the **** information recorded as a user's biological description data by the calculation function in a user authentication vote, only a different part from the 1st example using the drawing used for explanation of the 1st example is explained here.

[0075] CPU75, RAM76, etc. can be carried in the IC card used as a user authentication vote 7, and a fixed calculation function can be given to it. In the system of this example, if the user 8 who is going to use service inputs a user's biological information data in the authentication use place 4 using user authentication equipment 41, after changing this biological information data into the gestalt which carries out predetermined processing and is easy to carry out digital processing, it will send to the user authentication vote 7.

[0076] The user authentication vote 7 once memorizes the inputted information data to RAM76, and it compares and compares both, reading this information data and a just user's biological information data currently recorded on EEPROM79 by CPU75. Consequently, refusal is notified, if human being for whom both are in tolerance, are similar to, and are going to use service can attest the just owner of the user authentication vote 7, and success will be notified to the authentication use place 4 and it will not pass to this authentication.

[0077] The authentication use place 4 will provide a user 8 with desired service, if satisfied with the user authentication result of the user authentication vote 7. Furthermore, when you need prudent user authentication, it refers to the end certificate authority 3 or the middle certificate authority 2, and it judges together with the result. In addition, it cannot be overemphasized that the authentication use place 4 may serve as the end certificate authority 3. If what is similarly used for authentication of a low order level is having illustrated in the 1st example although the rate of distributing biological information data to every place was arbitrary at a big rate, the burden in a communication link becomes light and it is advantageous on employment of a system, and it is desirable to make the rate in the user authentication vote 7 60% or more.

[0078] Collapsibility use of the obstruction for participating in a system can be made easy to carry out low, since the burden on the operation of user authentication equipment 41 is mitigated, the cost of equipment can be reduced by utilizing the user authentication vote 7 which consists of a highly efficient IC card in this example and the costs needed for preparing the function of the authentication use place 4 become small. Moreover, since information processing is completed within a user authentication vote, as the memory of an authentication vote can be accessed from the outside, twist and read, an improper field is prepared, important information, such as authentication data, is recorded here and leakage is prevented, safety can be raised more.

[0079]

[Effect of the Invention] If the user authentication system of this invention is used as explained to the detail above When collating the biological description data in the **** information which a user inputs directly in an authentication use place, and an authentication vote and wanting a more advanced guarantee, in order to transmit a part of **** information to the certificate authority of a high order and to carry out user authentication, The user authentication corresponding to the demand level of safety can be obtained without performing the great portion of information processing in an authentication use

place, and covering a big load over a communication circuit. Moreover, construction of a very strong user authentication system is attained to invasion by dividing **** information.

[Translation done.]

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the user authentication system of the example of this invention.

[Drawing 2] It is the perspective view showing the example of the user authentication equipment used for this example.

[Drawing 3] It is the circuit block diagram of the user authentication equipment in this example.

[Drawing 4] It is the block diagram showing the example of a configuration of the user authentication vote used for this example.

[Drawing 5] It is the flow chart showing the example of a procedure which publishes the user authentication vote in this example.

[Drawing 6] It is the flow chart showing the example of a procedure of the authentication in the use place in this example.

[Description of Notations]

1 Qualification Registration Authority

11 Detachable Storage

2 Middle Certificate Authority

21 Storage

3 End Certificate Authority

31 Storage

4 Authentication Use Place

41 User Authentication Equipment

5 User Registration Place

51 **** Input Unit

52 Microphone

6 Authentication Vote Publishing Office

61 Authentication Vote Issue Equipment

7 User Authentication Vote

71 Connection Terminal

73 Non-contact Electrode

8 User

[Translation done.]

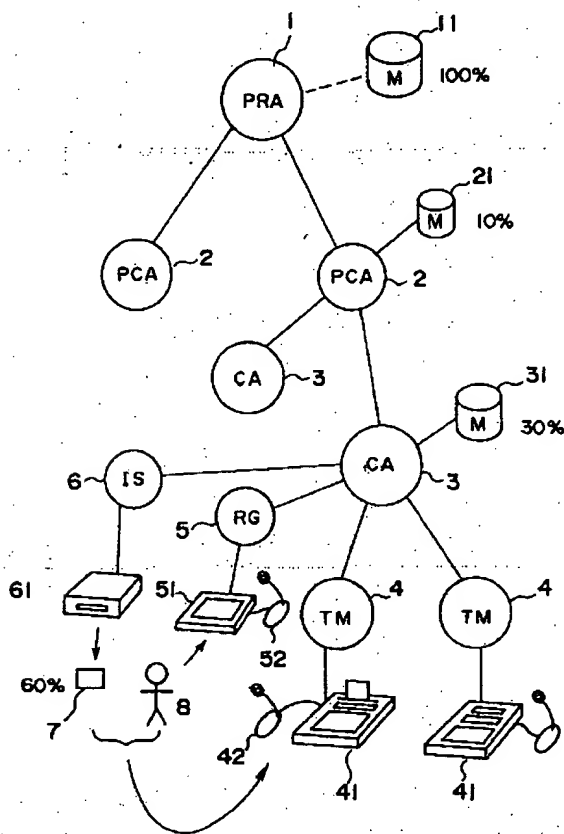
* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

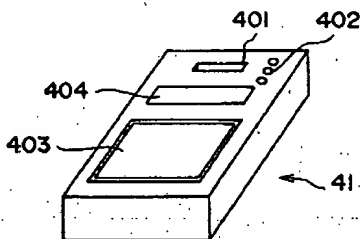
1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DRAWINGS

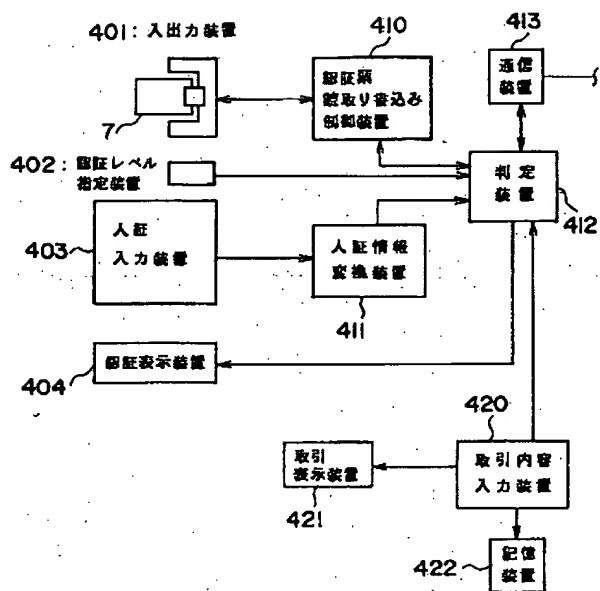
[Drawing 1]



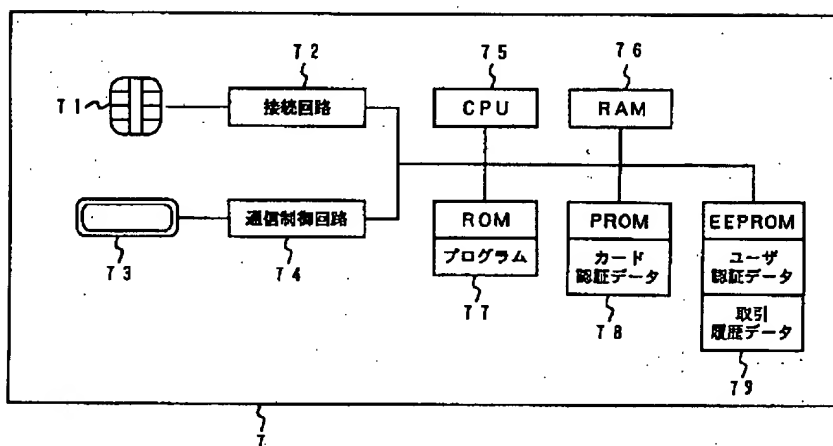
[Drawing 2]



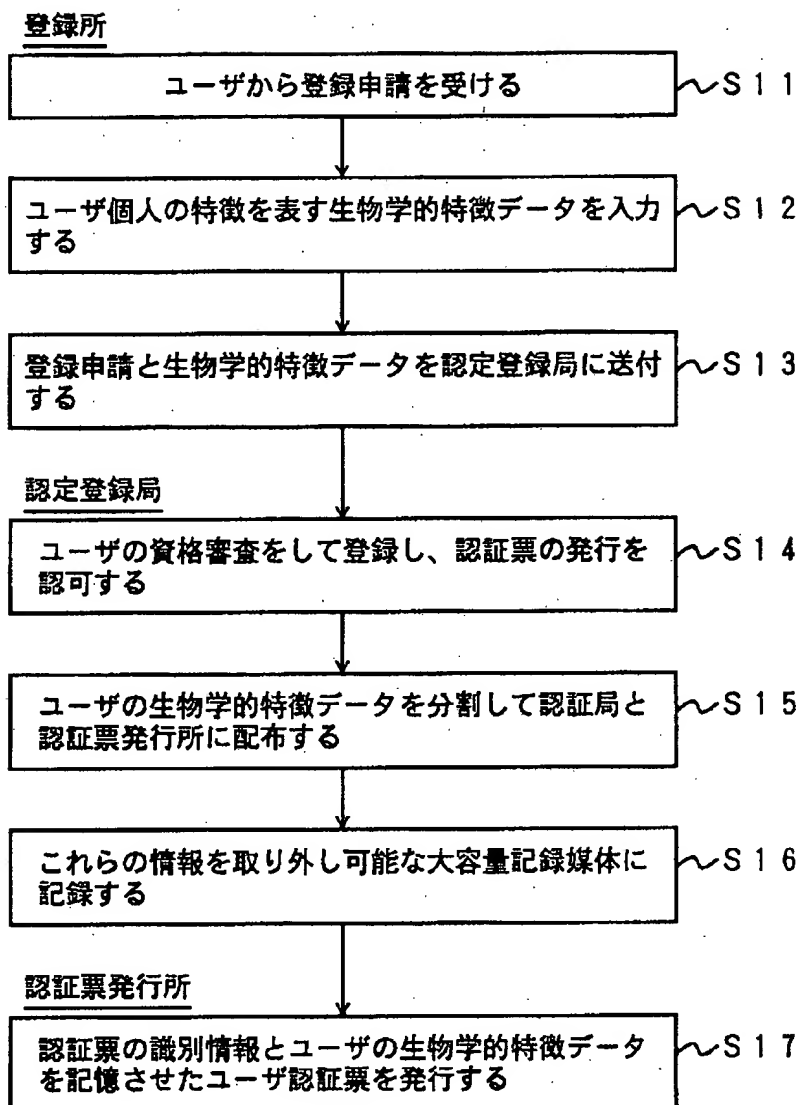
[Drawing 3]



[Drawing 4]

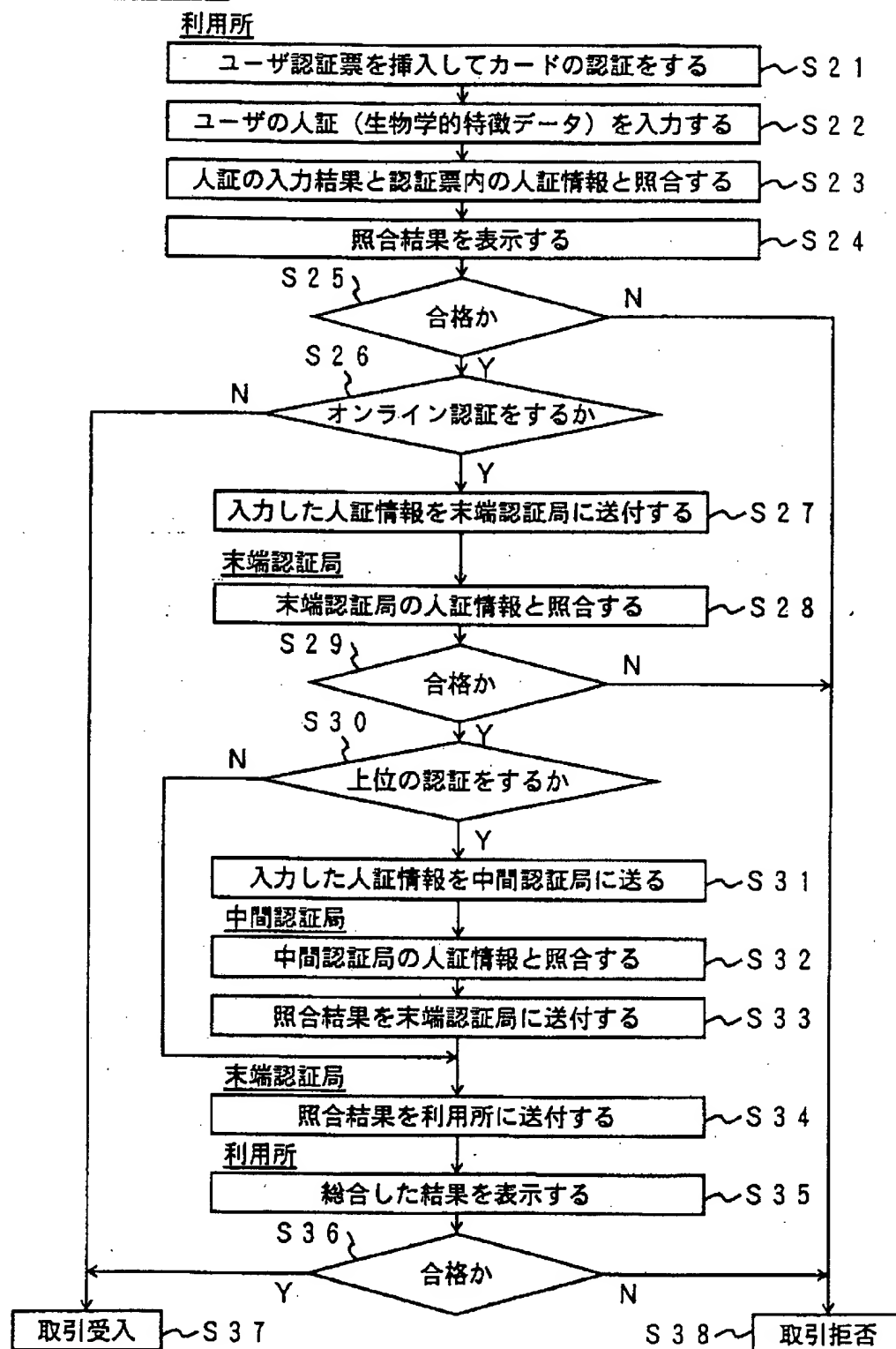


[Drawing 5]

ユーザ認証票の発行

[Drawing 6]

利用所における認証



[Translation done.]

(11)特許出願公開番号

(43)公開日 平成11年(1999)12月10日

(74)代理人 弁理士 関 正治

(2)

特開平 11-338826

1

2

【特許請求の範囲】

【請求項 1】 ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、該ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する認証票発行所と、該ユーザ認証票の情報を読み取る認証票読取り装置とユーザの生物学的特徴データを入力する人証取得装置を設けた認証利用所を備えてなるユーザ認証システムであって、該認証利用所において前記認証票読取り装置で読みとるユーザ認証票の記録内容と前記入証取得装置に入力された前記ユーザの生物学的特徴データを比較することにより該ユーザが該ユーザ認証票の正当な所有者であることを認証することを特徴とするユーザ認証システム。

【請求項 2】 ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、該ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する認証票発行所と、ユーザの生物学的特徴データを取得する人証取得装置と該取得した生物学的特徴データを前記ユーザ認証票に入力する人証情報書込み装置とを設けた認証利用所を備えてなるユーザ認証システムであって、前記ユーザ認証票に記録された生物学的特徴データの内容と前記入証取得装置で取得された前記ユーザの生物学的特徴データを前記ユーザ認証票の清算機能を用いて比較することにより該ユーザが該ユーザ認証票の正当な所有者であることを認証することを特徴とするユーザ認証システム。

【請求項 3】 前記ユーザ認証システムがさらに前記認証利用所と情報通信路で接続された少なくとも 1 個の認証局を備え、前記登録所において取得したユーザの生物学的特徴データのうち前記ユーザ認証票に記録しない部分を該認証局に記録しておいて、前記認証利用所からの照会に応じて前記ユーザ認証票において不足する生物学的特徴データの部分を比較して認証するようにしたことを特徴とする請求項 1 または 2 記載のユーザ認証システム。

【請求項 4】 前記情報通信路に流す情報は暗号化することを特徴とする請求項 3 記載のユーザ認証システム。

【請求項 5】 前記 2 個以上の認証局が、前記登録所において取得したユーザの生物学的特徴データのうち前記ユーザ認証票に記録しない部分を分割して記録しておいて、各認証局毎に前記認証利用所もしくは他の認証局からの照会に応じて自己の記憶する生物学的特徴データの部分を比較して認証するようにしたことを特徴とする請求項 3 または 4 記載のユーザ認証システム。

【請求項 6】 前記ユーザ認証システムが前記登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認証局を備えることを特徴とする請求項 1 ないし 5 のいずれかに記載のユーザ認証システム。

【請求項 7】 前記認証局における生物学的特徴データを記録した記憶媒体が該ユーザ認証システムの情報通信

路から切り離せることを特徴とする請求項 6 記載のユーザ認証システム。

【請求項 8】 前記生物学的特徴データが筆跡であることを特徴とする請求項 1 から 7 のいずれかに記載のユーザ認証システム。

【請求項 9】 前記生物学的特徴データとして複数のものを登録して、入力されたデータにより異なる取引を行うことを特徴とする請求項 1 から 8 のいずれかに記載のユーザ認証システム。

【請求項 10】 請求項 1 から 9 のいずれかに記載のユーザ認証システムに用いることのできるユーザ認証票であって、認識票を識別する信号とユーザの個体を区別する生物学的特徴データの少なくとも一部を記録した読出し可能な記憶領域を備えた記憶媒体からなるユーザ認証票。

【請求項 11】 さらに CPU と RAM を備えることを特徴とする請求項 10 記載のユーザ認証票。

【請求項 12】 前記記憶媒体が磁気記録媒体であることを特徴とする請求項 10 または 11 記載のユーザ認証票。

【請求項 13】 前記記憶媒体が IC カードであることを特徴とする請求項 10 または 11 記載のユーザ認証票。

【請求項 14】 ユーザ認証票に記録された情報を読み取る認証票読取り装置と、ユーザの生物学的特徴データを入力する人証取得装置と、前記認証票読取り装置で読み取ったユーザ認証票に記録されている生物学的特徴データと前記入証取得装置に入力された前記ユーザの生物学的特徴データを比較して合否を判定する判定装置と、判定結果を出力する表示装置を備えるユーザ認証装置。

【請求項 15】 前記入証取得装置が手書き図形取り込み機能を有するものであることを特徴とする請求項 14 記載のユーザ認証装置。

【請求項 16】 さらに、人証取得装置に入力されたユーザの生物学的特徴データの少なくとも一部を外部の認証局に送信し合否の判定結果を受け取る通信装置を備え、前記表示装置を介して判定結果を表示することを特徴とする請求項 15 または 16 記載のユーザ認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子情報交換や電子商取引における個人認証を行うためのユーザ認証システムと、これに用いるユーザ認証票、およびユーザ認証装置に関する。

【0002】

【従来の技術】近年、通信網を介してアクセスする情報の種類は極めて多様になりつつあり、商品の売買やクレジットなどの電子商取引は勿論、医療におけるオンライン診断や個人カルテ、役所における登録事項の閲覧、証明の発行など、対象もますます増加し、利用が進む傾向

(3)

特開平11-338826

3

4

にある。

【0003】こうした個人的な情報にはプライバシーに係わり他人に漏洩しないという保証がない場合には利用を認めるべきでないといわれるものが少なくない。電子情報通信網の発達を取り込んでより便利な情報社会を構築するために、個人を峻別できる信頼性の高いユーザ認証方式が求められている。また、個人を正しく認証する機構は、研究所や事業所あるいは住宅などにおける資格者以外の立ち入りを制限する施錠装置などや、電子マネーのセキュリティ向上にも利用することができる。

【0004】従来、ユーザ認証にはパスワードが最もよく用いられてきた。パスワードは簡便であるが、他人のパスワードを盗用して本人に成りすます者を排除することができない。このため、長いパスワードを使う、推測しにくいパスワードを選ぶ、パスワードを時々変更するなど、相応の注意をして安全性を確保しようとする。また、通信過程における安全性を確保するためには暗号化技術を用いて通信内容を秘匿化して、データの漏洩があっても他人に容易に内容を知られないようにすることも広く行われている。

【0005】しかしそれでも、通信の盗聴や暗号文の解読や盗み見などによりパスワードを盗まれることがあり、完全に安全なものとは成り得ない。また、パスワードを複雑にするほど利用者自身がそれを正確に記憶しておくことが困難になる欠点がある。さらに本質的には、どれほど複雑なデータであっても、それがデジタルデータとして蓄えられた瞬間から何らかの手段により複製することが可能になるという性質がある。

【0006】なりすましを防止し本人であることを確実に認証するため、指紋や声紋など、いわゆる生物学的特徴を表す情報を用いてユーザ認証する方法も検討されている。しかし、一般に生物学的特徴データは情報量が大きいので認証を必要とする利用現場とユーザの生物学的特徴を蓄積している認証局の間で膨大な通信量を交換しなければならない。したがって、通信路の輻輳や通信時間の長大化のため特殊な環境における場合以外には実用化することが困難であり、かつそのデータの管理場所と管理方法に問題があった。

【0007】

【発明が解決しようとする課題】そこで、本発明が解決しようとする課題は、電子情報交換や電子商取引における個人認証を行うための安全性が高く迅速に結果が得られるユーザ認証システムと、これに用いられるユーザ認証票およびユーザ認証装置を提供することである。

【0008】

【課題を解決するための手段】上記課題を解決するため、本発明のユーザ認証システムは、ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する

認証票発行所と、ユーザ認証票の情報を読み取る認証票読取り装置とユーザの生物学的特徴データを取得する人証取得装置を設けた認証利用所を備え、認証利用所の認証票読取り装置で読みとったユーザ認証票の記録内容と人証取得装置で取得したユーザの生物学的特徴データを比較することによりユーザ認証することを特徴とする。

【0009】また、本発明の第2のユーザ認証システムは、ユーザの生物学的特徴データを取得する情報取込み装置を備えた登録所と、ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する認証票発行所と、ユーザの生物学的特徴データを取得する人証取得装置と取得した生物学的特徴データをユーザ認証票に入力する人証情報書き込み装置とを設けた認証利用所を備え、ユーザ認証票の情報装置を用いて、記録されている生物学的特徴データの内容と人証取得装置で取得されたユーザの生物学的特徴データを比較することによりユーザ認証票の正当な所有者であることを認証することを特徴とする。

【0010】これら本発明のユーザ認証システムは、さらに、認証利用所と情報通信路で接続された少なくとも1個の認証局を備え、ユーザ認証票には登録所において取得したユーザの生物学的特徴データの一部を除いて記録しておき、ユーザ認証票に記録しない部分を認証局に記録しておいて、認証利用所からの照会に応じてユーザ認証票において不足する生物学的特徴データの部分を比較して認証するようにすることが好ましい。なお、情報通信路を介して相互に交換する情報は暗号化して安全性を保證することが好ましい。

【0011】また、2個以上の認証局があって、登録所で取得したユーザの生物学的特徴データのうちユーザ認証票に記録しない部分を分割して記録しておいて、各認証局毎に認証利用所もしくは他の認証局からの照会に応じて自己の記憶する生物学的特徴データの部分を比較して認証するようにすることがより好ましい。さらに、ユーザ認証システムには登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認証局を備えてもよい。また、認証局における生物学的特徴データを記録した記憶媒体はユーザ認証システムの情報通信路から切り離せるようになっていることが好ましい。なお、生物学的特徴データとして筆跡を用いてもよい。

【0012】本発明のユーザ認証システムは、ユーザの個体を区別する生物学的特徴データの少なくとも一部を記録したユーザ認証票を使用して、ユーザが入力した生物学的特徴データとユーザ認証票の生物学的特徴データを比較することによりユーザ認証するため、ユーザ自身でなければ認証テストをパスすることができないので、パスワードの窃取によるなりすましを防止できる。

【0013】また、デジタルデータ化された生物学的特徴データから元の生物学的特徴データを復元することは極めて難しいばかりか、たとえ復元ができてその生物

(4)

特開平11-338826

5

学的特徴を他人が複製することはできないため、ユーザ認証の信頼性が極めて高い。特に、ユーザ認証票に照会用の生物学的特徴データを記録しているため、遠隔の認証局でユーザ認証をしてもらわなくても、認証を必要とする認証利用所において本人であることを直接確認することができる。このため認証局との通信に多大な時間および費用を費やす必要がない。

【0014】なお、ユーザ認証は、ユーザ認証票に記録した照会用の生物学的特徴データと認証利用所で入力させたユーザの生物学的特徴データとの対照を認証利用所に設けた論理演算装置で行うこともできるが、ユーザ認証票内にCPUやRAMなど演算機能を備えて、ユーザ認証票を利用しようとするユーザから取得した生物学的特徴データを入力し記録されている情報と対照するようにしても良い。ICカードなど高度な機能を有するユーザ認証票を活用することにより、認証利用所の負担を軽減し装置コストを低減し、システムとしてより利用しやすいものとすることができる。また、このようにユーザ認証票内で情報処理を完結させることにより認証票の外部に認証データが漏洩するのを防いで安全性を向上させることができる。

【0015】さらに、認証利用所と情報通信路で接続された認証局にユーザの生物学的特徴データのうちユーザ認証票に記録しない残りの部分を記録しておいて、認証利用所からの照会に応じて生物学的特徴データの部分を比較して認証するようにする場合は、必要情報を分割して記憶しておくので、例えば認証票に記録されたデータから生物学的特徴データを復元しても認証システムを突破することはできないし、認証票から認証に用いるデータを複製することもできない。また、たとえ認証票の記憶内容を改竄しても認証局における情報が保全されているため他人のなりすましを排除することができる。あるいはまた、認証局がアタックされた場合にもユーザの所有するユーザ認証票の情報まで改竄することができないため安全である。なお、情報通信路に流す情報が暗号化されたものであれば、通信路の途中で情報を窃取する者があっても解読しにくい為安全性が向上する。

【0016】また、ユーザ認証票と2個以上の認証局でユーザの生物学的特徴データを分割して記録しておいて、ユーザ認証票の情報に基づいたユーザ認証に加えて、各認証局毎に認証利用所もしくは他の認証局からの照会に応じて記憶する生物学的特徴データの部分を比較して認証するようにした場合は、例えば階層的に組織された認証局のユーザ認証を段階的に取得することによりユーザ認証の信頼性をより高くすることができる。

【0017】なお、本発明のユーザ認証システムでは、要求される認証信頼性のグレードに従い、ユーザ認証票に記録された情報に基づく認証利用所のみで認証を台否決定することを選択しても、ユーザ認証票には記録されていない情報を加味した1個または複数の認証局にお

6

る認証を追加してより確実な判定を選択してもよい。たとえば低額の商品を取引する場合はそれほど慎重にユーザ認証を行う必要がないのに対して、高額な商品を取り扱う場合はより高度な保証が必要であるし、病院のカルテなどのように高度のプライバシーに係わるものを扱う場合は確実に本人の請求であるかを確認する必要がある。

【0018】このような認証の安全性に対するレベルは認証利用所や取引対象により予め決めておいてもよく、取引毎に認証利用所で設定してもよい。さらに、取引価額などに伴い自動的に選択して設定できるようにしてもよい。また、この情報分割方式によれば、たとえ生物学的特徴データの全部を用いてユーザ認証を行う場合でも、大部分はユーザ認証票中の情報を用いて認証利用所で認証を行うため、通信回路を介して交換する情報量は小部分であるから、通信回路容量も小さくてよくまた照会に掛かる時間も少ない。なお、情報を分割することは、多数のユーザについて情報を集積しておき多数の照会を処理しなければならない認証局における処理能力や記憶容量の要求を抑制する効果もある。

【0019】さらに、ユーザ認証システムには登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認定登録局を備えて、登録所において取得したユーザの生物学的特徴データの全容を記録しておくことにより、何らかの不正使用や異常が起きた位置の判定、あるいは認証票が破損したときの再発行、下位の認証局のデータの補修などに利用することができる。

【0020】また、認定登録局における生物学的特徴データを記録した記憶媒体がユーザ認証システムの情報通信路から切り離せるようにしておいて必要なときだけ接続して使用するようにすれば、ハッカーの侵入などにより個人情報に漏洩したり改竄されたりすることを防止することができる。なお、ユーザ認証票や下位の認証局にはそれぞれ部分的な生物学的特徴データのみを記録し完全な記録を残さないようにすることが安全性を確保するために極めて有効である。

【0021】本発明のユーザ認証システムで使用する生物学的特徴データとして筆跡を用いてもよい。筆跡は個人の生物学的特徴をよく表して他人のなりすましが難しく、かつ入力する装置および解析する装置が比較的容易に得られるという利点がある。ユーザを識別するために書いて貰う文字や図形は適当なものでよいが、自己の氏名を表すサインなどは再現性がよいので好ましいとはいってもない。また、利用可能な生物学的特徴データには、この他、指紋や掌紋、声紋、虹彩や網膜のパターン、DNA情報などがある。今後もより確実で容易に認識できる生物学的特徴が見出される可能性がある。

【0022】なお、ユーザ認証票と認証局で生物学的特徴データを分割して記録する場合に、情報データを物理的に分割して前半部分をユーザ認証票に記録し、後半部分を認証局に記録して照合するようにしてもよく、ま

(5)

特開平11-338826

7

た。例えば掌脈の形状情報をユーザ認証票に記録し、掌圧情報や掌順情報を認証局に記録するなど、情報を階層的にとらえて分割する方法を用いてもよい。さらに、サインと声紋など複数の生物学的特徴データを別々に記録し、それぞれ異なる種類の情報に基づいて判断することにより信頼性を向上させることも可能である。

【0023】なお、生物学的特徴データとして複数のものを登録して、入力されたデータにより異なる取引を行うように構成しても良い。正規の生物学的特徴データの他に、特殊な意味合いを持たせた情報を複合して用いるようにすれば、例えば、他人に脅かされて意志に反してサインをせざるを得ない事態に陥った場合にサインのどこかに隠し記号を付け加えると、強要者には素直にサインをしているように見せかけて実は警備会社に通報をするといった仕組みにすることもできる。

【0024】なお、システム構築上の選択として、このような場合に人身上の安全を確保するため、扉の開閉や現金の引出など普通に取引が成立しているように見せかけるようにすることも可能である。勿論、こうした目的に使用する生物学的特徴データは正式なものと同じ種類のものであっても良い。例えばサインに対して音声データを付加するなど異なる種類のものを複合しても良い。また、逆に、疑似データに特定の符号データを付加したものを正式な認証用データとしても良い。

【0025】なお、上記課題を解決するため、本発明のユーザ認証票は、認証票を識別する信号とユーザの個体を区別する生物学的特徴データの少なくとも一部を記録した読出し可能な記憶領域を備えた記憶媒体からなることを特徴とする。記憶媒体として、ROMやCD-ROMなど読み取り専用の記録媒体を使用してもよいが、記録内容が使用者の生物学的特徴を衰す情報であるため改竄の危険が小さいので、取引内容や新たな情報を追加して記録できる書き込み読み取り共に可能な記憶媒体であることも可能である。

【0026】特に高い偽造防止機能と大きなデータ容量を有し、インテリジェント機能と暗号システムを搭載したセキュリティ機能が高いICカードを利用することが好ましい。また、CPUやRAMを搭載したICカードを用いる場合は、ユーザから取得した生物学的特徴データをカード内に取り込んで、内部に記憶した照会用データと比較してユーザ認証を行うようにすれば、認証利用所の負担を軽減し装置コストを低減することができる。また、外部からユーザ認証票の認証データを読み出せないようにして安全性を向上させることができる。

【0027】なお、ICカードを使用することにより複合的な機能を搭載し高度な本人認証機能を有する多目的カードにすることができる。ここで使用するICカードは、外部端子により読み書きする接触式と外部端子によらず非接触で読み書きする非接触式を複合した複合ICカードであってもよい。本発明のユーザ認証票は、特に

8

情報を分散して用いる場合は、記録内容を改竄しても役に立たないので、より経済的で簡便なフロッピーディスクを使用してもよい。また、この他にも、CD-ROM、DVD、録音テープ、MD等、書き込み可能な各種の記録媒体が使用できる。

【0028】また、上記課題を解決するため、本発明のユーザ認証装置は、ユーザ認証票に記録された情報を読み取る認証票読取り装置と、ユーザの生物学的特徴データを取得する人証取得装置と、認証票読取り装置で読み取ったユーザ認証票に記録されている生物学的特徴データと人証取得装置で取得したユーザの生物学的特徴データを照合して合否を判定する判定装置と、判定結果を表示する表示装置を備えることを特徴とする。

【0029】本発明のユーザ認証装置によれば、ユーザ認証票を認証票読取り装置にかけると共に、認証を求められたユーザが人証取得装置を介してユーザ認証票に記録されたものと同じ種類の生物学的特徴データを入力すると、判定装置がユーザ認証票に記録された生物学的特徴データと人証取得装置で取得された生物学的特徴データを照合して合否を判定した結果を表示装置に表示するので、外部と通信をしなくても直ちにユーザ認証票の真正な所有者であるか否かを認知することができる。

【0030】なお、ユーザ認証装置にはユーザ登録所に設置される生物学的特徴データ入力装置と同じ種類の人証取得装置を備える必要がある。人証取得装置として手書き図形取り込み機能を有するものを使用することができる。手書き図形取り込み機能を利用して、サインなど予め決めた任意の手書き図形をデジタルデータとして入力すれば、ユーザ認証票の生物学的特徴データと比較することが容易に可能となる。

【0031】さらに、本発明のユーザ認証装置は外部の認証局と通信できる通信装置を備え、人証取得装置に入力されたユーザの生物学的特徴データの少なくとも一部を外部の認証局に送信し合否の判定結果を受け取り、表示装置を介して判定結果を表示するようになっていることが好ましい。外部の認証局と接続して認証データを階層的に扱うことにより、悪意を持つ侵害者のアクセスや改竄を防止し、より安全性の高い認証能力を備えることが可能となる。

【0032】

【発明の実施の形態】以下、図面を参照して本発明の詳細を実施例に基づいて説明する。図1は本発明のユーザ認証システムの1実施例を示すブロック図、図2は本実施例に使用するユーザ認証装置の例を示す斜視図、図3はユーザ認証装置のブロック図、図4は本実施例に使用するユーザ認証票の例を示すブロック図、図5は本実施例におけるユーザ認証票を発行する手順例を示す流れ図、図6は利用所における認証の手順例を示す流れ図である。

【0033】

(5)

特開平11-338826

9

10

【実施例1】本実施例のユーザ認証システムは、図1にあるように、認定登録局、認証局および認証利用所からなる階層構造を有する。認定登録局（PRA）1は認証ネットワーク全体を統括するもので、ライセンサーとしての複数の中間認証局（PCA）2に一部の権限を与える証明書を発行し、権限を授けられた中間認証局がサブライセンサーとしての複数の末端認証局（CA）3に一部の権限を与える証明書を発行する。

【0034】末端認証局（CA）3が、ユーザ認証を利用するクライアントとなる認証利用所（TM）4とクライアントのサービスを利用しようとするユーザ8を仲介する機関となる。なお、以下の説明において各種サービスの利用を取引と表現する場合がある。なお、認定登録局（PRA）1は装置から切り離すことができる記憶装置11を備え、中間認証局（PCA）2と末端認証局（CA）3は装置に常時接続されている記憶装置21、31を備えている。

【0035】これらの機関はそれぞれ専用回線や公衆回線により接続されていて、随時情報の交換ができるようになっている。なお、イントラネット網やインターネット網を利用した通信によってもよい。これら通信回線を用いて情報を交換するときは公開鍵や共通鍵を用いた暗号化処理を行うことにより安全を確保するようにすることが好ましい。なお、中間認証局（PCA）はユーザ認証システムを構築する上で省略が可能である。また、中間認証局（PCA）を多段に備えて階層の深さが3段より大きくなっていてもよい。なお、認定登録局（PRA）、中間認証局（PCA）、末端認証局（CA）などの機能は相互に合体した機関が実行するようにしても良いことは言うまでもない。

【0036】末端認証局（CA）は、一般には、行政機関、医療機関、特定企業、共同住宅、商店街（モール）など、対象を限った領域についての権限を認定登録局（PRA）や上位の認証局（PCA）から授与されている。末端認証局（CA）3には、この権限を有する領域に属しユーザ認証を利用する認証利用所（TM）4が接続されている。

【0037】認証利用所（TM）4に該当するものには、役所の各窓口、病院の各科受付や薬局受付、研究所や部課の扉、保護を必要とするデータベースにアクセスする情報機器、マンション入口や個室の扉、室内ユーティリティの遠隔操作装置、会員制クラブの施設、モールの各店舗やデパートなど大型小売店の支払窓口、銀行など金融機関の窓口や自動支払機など、各種のものがある。特にダイレクトマーケティングにおけるユーザ認証は今後さらに重要な課題となり、各ユーザ8の自宅に認証利用所4を設置する状況も考えられる。

【0038】末端認証局（CA）3は、認証利用所（TM）4を利用しようとするユーザ8を対象として登録の受付をする権限をユーザ登録所（RG）5に与え、また

認証票発行所（IS）6にユーザ認証票7の発行を行う権限を与える。

【0039】ユーザ登録所（RG）5には、生物学的特徴を取得する入力装置51が備えられている。本実施例ではタブレットとペンから成るオンライン手書き図形入力装置を利用している。オンライン手書き図形入力装置から筆跡を入力すると、筆記過程の情報を一緒に取り込んで図形認識することができるので、例えば文字を入力したときにも筆画それぞれがどのような方向にどの順序でかけられたかの情報なども容易に取得できる。

【0040】また、生物学的特徴をとらえる手段として声紋を利用する場合はマイクロホン52を装着して音声を入力する。なお、指紋や掌紋を取り込む装置や、瞳を観察して虹彩や網膜パターンを取り込む装置を備えてもよい。これら入証手段を複数併用することにより、入証をより確実にすることもできる。

【0041】認証票発行所（IS）6には認証票発行装置61が設置されている。認証票発行装置61は、ユーザ認証票7に入定に用いられる情報を書き込んでユーザ8に給付する。本実施例におけるユーザ認証システムでは、ユーザ認証票をICカードで構成したが、書き込み読み出し可能な記録媒体であればよく、CD-ROM、フロッピーディスクや磁気カードなど磁気記録媒体、あるいは光磁気記録媒体等、他の電子記録媒体を使用することもできる。

【0042】認証利用所（TM）4には、ユーザ8が持っているユーザ認証票7の真正を検査しユーザ8の認証を行うユーザ認証装置41が設けられている。図2と図3はユーザ認証装置41の1構成例を示す図面である。ユーザ認証装置41の上面には、認証票7を挿入するスロットがあって挿入された認証票7の記憶領域と情報をやり取りする入出力装置401と、取引に要求される認証の深さを指定する認証レベル指定装置402と、ユーザの生物学的特徴データを取得する入証入力装置403と、認証結果を表示する認証表示装置404が配置されている。

【0043】なお、入証入力装置403は、ユーザ登録所（RG）5で用いられる生物学的特徴入力装置51と同じものである。従って、ユーザ認証に声紋を併用する場合には、認証利用所（TM）4のユーザ認証装置41にもマイクロホン42を付設する必要があることはいうまでもない。このように入証入力装置403は、利用するユーザの生物学的特徴データの種類に従ってそれを取得するために適合する入力装置を備えている。

【0044】また、ユーザ認証装置41の内部には、これら装置を有機的に結合してユーザ認証を行う電子回路410が内蔵されている。この電子回路410は、認証票読取り音込み制御装置411と入証情報変換装置412と判定装置413と通信装置414から構成されている。認証票読取り音込み制御装置411は、入出力装置

11

401を介して認証票の記録内容を読み取り暗号化されたデジタルデータを復号化した認証票に取引結果を記憶させる機能を備えている。

【0045】また、人証情報変換装置412は、人証入力装置403で取り込んだ生物学的特徴データをデジタルデータに変換する。判定装置413は、認証票読取り書込み制御装置411と人証情報変換装置412と認証レベル指定装置402の出力情報を取り込み、必要とされる認証レベルに従って通信装置414を介して認証局とやり取りした情報を加味してユーザの個人認証を行

い。結果を認証表示装置404に表示させる。
【0046】ユーザ認証が行われて取引が成立すると取引結果が取引内容入力装置420から入力され、その内容は取引表示装置421に表示されるので、ユーザもこれを確認することができる。また、取引の内容は記憶装置422に記録される。なお、判定装置413がユーザ認証結果を自動的に取引内容入力装置420に送り、取引の受入あるいは拒否ができるようにしてもよい。

【0047】さらに、取引内容入力装置420から取引情報を入力してユーザ認証票7に取引内容や取引履歴を記録するようにしてもよい。例えばユーザ認証票7を決済分野に使用する場合は取引日と購入商品名と価額を記録しておけば支払い時における対照確認が容易になる。また行政サービス用の認証票では健康保険証や運転免許証、医療情報あるいは住民基本台帳などの証明書類をユーザ認証票7の中に受領して保存するようにすることもできる。また、ユーザ認証票7に記録された内容を閲覧するときにユーザ認証を条件とすることにより本人以外のアクセスを排除して、個人のプライバシーを保護することができる。

【0048】なお、正しい認証に用いるための生物学的特徴データの他に、特殊な意味合いを持たせた情報を複合して用いるようにしてもよい。例えば、強盗や脅迫者などに脅かされて意志に反してサインをせざるを得ない事態に陥った場合に、正規のサインに何気なく隠し記号を付け加えると、扉の開閉や現金の引出など普通に取引が成立するが、同時に警備会社にも通報が行っていて、利用者の安全が確保された状態になったところで犯人を逮捕するなど、適当な処置を執るようになる仕組みを持たせるようなこともできる。こうした目的に使用する生物学的特徴データとして、例えばサインすると同時に軽く2回核押しするなど、異なる種類のものを複合して用いてもよい。

【0049】図4は、ICカードを使用したユーザ認証票の内部構成を示すブロック図である。本実施例で用いられるユーザ認証票7は、複数の発行者が共同で共用端末を設置し相互解放するための便宜を考慮して、接続端子71を介して電気信号を伝達する接触型と、カード内の電極73と認証票読取り書込み制御装置内の電極が接触しないで静電結合や電磁誘導などにより通信する非接

(7)

特開平11-338826

12

触型との両方を備えた複合型ICカードを採用するが、いずれか一方の方式を設備したものであってもよい。

【0050】接続端子71には接続回路72、非接触電極73には通信制御回路74が接続されていて、内蔵するメモリと連結されている。ユーザ認証票7は、ランダムアクセスメモリRAM76と読み出し専用メモリROM77と電気的に書込み可能なプログラム可能読取り専用メモリPROM78と電気的に消去可能なプログラム可能読取り専用メモリEEPROM79からなるメモリとCPU75を備えていて、相互間はバスにより接続されている。接続回路72と通信制御回路74とCPU75およびメモリは1個のICチップに収容することができる。

【0051】認証票読取り書込み制御装置411は、ユーザ認証票7が挿入されると接続端子71から接続回路72を介し、または非接触電極73から通信制御回路74を介して、ユーザ認証票7のメモリにアクセスすることができる。PROM78には認証票の真正性を検査するために使用するカード認証データや証明を受けてユーザ認証票を発行した発行者を明らかにするIDなどが格納され、一旦書き込んだデータは書き換えることができない。EEPROM79にはユーザの認証に用いる生物学的特徴データや認証票を用いた取引の記録が格納される。またROM77にはCPU75を制御して、暗号化や復号化、データ入出力の管制、ユーザ認証装置41の真正性検査などを行うプログラムが格納されている。RAM76は外部から取り込むデータや演算過程で必要となるデータを一時保持する機能を有する。

【0052】ユーザ認証票7は認定登録局1でシステムに使用される適正なカードであることが保証できる正しいカード認定情報をPROM78に書き込んだ状態で各認証票発行所6に配布されている。従って、認証票発行所6は認定登録局1からの指示に基づいてユーザの生物学的特徴データの一部をEEPROM79に書き込めばよい。カードの改竄を認めないようにするために、認証票発行装置はPROM78の書き換え機能を備えないようにしても良い。ただし、本実施例における認証票のメモリ配分は上記に限られず、例えば本人認証を行うための生物学的特徴データをPROM78あるいはRAM76に記録しても良い。

【0053】図5を用いてユーザ認証票を発行する手順の1例を説明する。ユーザ登録所5は、その管轄領域内の認証使用所4のサービスを受けることを欲するユーザ8から登録申請を受け付ける(S11)。この時ユーザ登録所5は必要に応じてユーザ8の資格審査に用いる情報を読取するとともに、ユーザ個人の生物学的特徴を表す情報を取得する(S12)。ここで利用する生物学的特徴はユーザ個体に特有であって、他人が模倣や変装などによりそのユーザになりすまそうとしても見做ることができるような性質を有するものが選択される。

13

【0054】本実施例では、筆跡を用いて識別するようにしている。入力する図形は任意でよいが、ユーザ8が入力する度に異なるのは認証を行う上で具合が悪いので、普通は、再現性を保証するため自己の氏名を表すサインを入力させるのが好ましい。なお、複数の生物学的特徴を用いると認証の安全性が向上するため、補助的にマイクロホン2を用いて声紋も取得できるようにしてある。ユーザ登録所5で採取された申込人の資格情報と生物学的特徴データは認定登録局1に伝送される（S13）。

【0055】認定登録局1は、ユーザ登録所5から受け取った情報に基づいて資格審査をし、合格した者に対して認証票の発行を許可する（S14）。資格条件は認証を利用する対象に従って決まるので、実際にユーザを受入れる末端認証局3で審査するようにしてもよい。認定登録局1は、登録ユーザ8の生物学的特徴データを所定の割合に従って階層的に分割し、ユーザ認証票7と各段階の認証局2、3に分配する部分を決定して各所に配布する（S15）。

【0056】認定登録局1で各所に分配された生物学的特徴データは、認証利用所4の要求する認証精度に基づいてアクセスするものであり、最も低度の信頼性で足りる場合は認証利用所4の認証装置41で対照した結果だけで認証できるようにし、中度の信頼性を要求するときは末端認証局3に格納された情報を加味してユーザ認証し、最も高度の保証を要求する場合は分散格納された全ての生物学的特徴データを統合して判定するようにする。

【0057】本発明のユーザ認証システムでは、生物学的特徴データは初めに認証利用所4で真正性を検査して合格したときだけ上位機関の認証を請求できるように構成する。上位の認証機関ではユーザ認証票7にない部分の情報を用いた認証を行う。従って、ユーザ認証票7には最小限ユーザ8が入力する生物学的特徴データと対比することによりある程度の確度で真正ユーザであることが判断できる情報を配分しておかなければならない。

【0058】本実施例では約60%の情報をユーザ認証票7に分配し、末端認証局3に30%の情報、中間認証局2に残りの10%の情報を分配することとした。このように級数的に情報量を減少させることで、より多数の認証請求が集まる上位機関の記憶容量を節約し、かつ認証に要する時間負荷を減少させる効果が生じ、システム全体としての情報保護性能の向上を図ることができる。

【0059】なお、より高度な保証を要請されたときに上位の機関に送達する情報が過大にならないためには、ユーザ認証票7に保持する生物学的特徴データの割合がある程度大きい方が好ましい。しかし、ユーザ認証票7に与える情報の比率が過大になるとユーザ認証の信頼性が低下する。従って、生物学的特徴データの分配に当たっては、接続するユーザ数や要求される認証の安全性な

(8)

特開平11-338826

14

どを勘案し、実際の条件に適合した適切な分割割合を定める必要がある。

【0060】情報の分割方法は、デジタル情報化されたデータを所定の割合で物理的に分割する方法であってもよいが、また筆跡のように描き終わった形状に関する情報と描いている途中の筆勢に関する情報、さらに筆順などの情報というように段階を追った情報として分割してもよい。例えば、声紋を周波数帯に分割したり指紋を指毎に分けてそれぞれに記録して利用するなど、生物学的特徴は、いずれも適当に分割して利用することができる。なお、筆跡と声紋など複数の特徴を取得して異なる種類ごとに分割して用いてもよい。

【0061】認定登録局1は、認証票とユーザに関する情報を磁気テープやCD-ROM、光磁気ディスク、DVD、あるいはリムーバブルハードディスクなど、装置から切り離すことができる大容量の記憶手段11に記録して保存し（S16）、下位機関から要請があったときに係員が再生装置に装着して登録された情報を照会するようにする。認証登録局1では、取り外し可能な記録装置11を用いて、情報記録媒体11は不要時には外部の通信回路網から切り離して保管するので、外部からの侵襲や改竄を防止することができる。

【0062】認証局2、3に配布された個人の生物学的特徴データはそれぞれに付属する記憶装置21、31に格納され必要に応じて随時読み出して利用する。認証票発行所6は、認証票毎に決められたカード認証暗号が記録されているユーザ認証票7に認定登録局1から分配を受けた登録申込人の生物学的特徴データを記録してユーザ8に支給する（S17）。

【0063】なお、1個の末端認証局（CA）3に複数のユーザ登録所（RG）5と認証票発行所（IS）6を備えてもよい。ユーザ8はユーザ登録所5に出頭して実際に自身の生物学的特徴を入力しなければならないので、発行されたユーザ認証票7を受け取る認証票発行所6がユーザ登録所5と同じ場所に設置されているとユーザ8の便宜のために好ましい。

【0064】なお、ユーザ8の入定のため信頼がおける人物の立会を条件とするようにしてもよい。ただし、初めから他人になりすましている場合を完全に排除することはどの様な機構を用いても困難である。また、登録するユーザが申告した事実を確認するためには、登録手続と同時に認証票を発行する方式でなく、後に住所に郵送する方式を採用してもよい。なお、認定登録局（PRA）1がユーザ登録所（RG）5と認証票発行所（IS）6を備えるようにしてもよい。さらに、ユーザ登録所（RG）5と認証票発行所（IS）6の機能を備えた携帯用端末を持った発行者が任意の場所において登録発行手続をすることも可能である。このような携帯用端末の利用は認定登録局（PRA）から正規の資格認定を受けた者しか認めないようにはする必要があり、ここでも発

15

行者としての厳重な認証を受けて始めて操作できるように構成されている。

【0065】次に、図6を用いて、認証利用所4においてユーザ認証票7によりユーザ認証をする手順の1例を説明する。ユーザ8がユーザ認証票7を提出して認証利用所4に取引を申し出ると、認証利用所4はその認証票7を認証装置41のカードスロット（入出力装置）401に挿入して認証用の情報を読み取る。認証用の情報にはカードの真正性を確認するための情報とユーザ認証のための生物学的特徴データが含まれる。

【0066】認証利用所4は初めにカードの認証を行う（S21）。カードの認証は、ユーザ認証票7が認証利用所4が使用するユーザ認証システムに適合する真正なものであり正当な所持者が誰であるかを確認することである。対応しない認証票を使用している場合は初めから取引を受け付けない。なお、逆にユーザ認証票7が不正にアクセスされていないことを確認するために、ユーザ認証票7中のプログラムにより認証装置41が自身の認証票と対応するものであるかを検証して、正しい認証装置でない場合は記憶内容の開示を拒絶する仕組みを備えてもよい。

【0067】カード認証で合格したときには、ユーザ8にタブレット（入証入力装置）403上にサインを書いて貰うなど、ユーザ認証票7を取得したときに用いたものと同じ生物学的特徴を表示することを求める（S22）。そして、タブレット403から入力した生物学的特徴データをユーザ認証票7に記録されていた例えば60%の生物学的特徴データと照合して、窓口のユーザ8がユーザ認証票7の真正な所持者か否かを判定する（S23）。ユーザ認証結果は表示装置404に表示する（S24）。

【0068】認証利用所4におけるユーザ認証の合否に従い手順が異なる（S25）。ユーザ認証が否定されたときは認証利用所4は取引を拒絶する（S33）。ユーザ認証に合格したときはさらに上位の認証機関にオンライン認証を求めるべきか否かを調べる（S26）。オンライン認証を必要としない場合は直ちに取引の申し出を受け入れてよい（S32）。オンライン認証の要求の有無や深さの要求度は取引毎に認証レベル指定装置402からオペレータやユーザ8が入力してもよいが、取引の性格や取引金額の多寡に基づいて自動的に設定されるようにしてもよい。

【0069】オンライン認証を必要とする場合は、認証レベルの要求と共にユーザ認証票7の情報と入証入力装置403で取得した入証情報とを末端認証局3に送付する（S27）。送付する入証情報は、認証利用所4で利用した部分を除外した例えば40%の部分でよいから、認証利用所4と末端認証局3の間で交換する情報量を削減することができる。

【0070】オンライン認証の要否は、取引の性格に従

(9)

特開平11-338826

16

った認証の安全性に対する要求水準により決められる。換金性の高い商品や高額商品の取引とか個人の秘密情報の開示にはより安全な認証が必要とされるので、上位機関のユーザ認証が求められることになる。また、認証利用所4の性格によってオンライン認証の深さが指定される場合もある。病院の窓口などではプライバシーの保護と正確な治療行為を保证するため高度な本人認証が必要とされる場合が多い。なお、通信回線を使った在宅診療などでは確実に本人のデータであることを確認するため、上位の認証局までユーザ認証を求めるようにすることが好ましい。

【0071】末端認証局3では記憶装置31に記録されているユーザ8の固有の入証情報と照合して（S28）、認証結果を認証利用所4に回付する（S29）。末端認証局3にはユーザの入証情報の30%しか記録されていないので、ここにおけるユーザ認証だけでは不足する場合は、さらに上位の中間認証局2にユーザ認証を求める。中間認証局2には各ユーザについて10%の生物学的特徴データを記録してあるので、認証利用所4で取得した入証情報のうち中間認証局2で使用する部分は10%になり、末端認証局3から中間認証局2に送付すべき情報量はさらに大幅に減少する。中間認証局2で行ったユーザ認証結果は末端認証局3を介して認証利用所4に戻る。

【0072】各所のユーザ認証結果は認証利用所4で総合されてユーザ認証装置41の認証表示装置404に表示される。ユーザ認証が合格の場合は取引を受け入れ（S32）、不合格の場合は取引を拒否（S33）することになる（S31）。また、ユーザ認証が否定されたときは改ざんやなりすましなど何らかの不正行為の可能性もあるので、その情報を認定登録局1まで送付して問題の在処を確認して原因の解析を行うことが好ましい。

【0073】認定登録局1には外部から侵入したり改ざんすることが困難な記録が保管されているので、認証利用所4における入力データと対比することにより、異常がユーザ認証票7にあるのか、末端認証局3にあるのか、あるいは中間認証局2にあるのかが明確になる。ユーザ認証票7の内容とユーザ8が入力した情報の間に齟齬がある場合は盗難や拾得により真正でないユーザが使用している場合やユーザ認証票のデータが不当なアクセスにより書き替えられた場合が考えられる。

【0074】

【実施例2】本実施例のユーザ認証システムが第1の実施例と異なる点は、認証利用所に設けた論理演算装置でユーザ認証票に記録した生物学的特徴データと入証取得装置で入力させたユーザの生物学的特徴データとを対照して行う代わりに、ユーザ認証票内の演算機能によりユーザの生物学的特徴データと記録された入証情報とを対照するようにした点のみであるので、ここでは、第1実施例の説明に使用した図面を用いて第1実施例と異なる

50

(10)

特開平11-338826

17

部分についてのみ説明する。

【0075】ユーザ認証票7として使用するICカードには、CPU75やRAM76などを搭載して一定の演算機能を持たせることができる。本実施例のシステムでは、認証利用所4でサービスを利用しようとするユーザ8がユーザ認証装置41を用いてユーザの生物学的情報データを入力すると、この生物学的情報データを所定の処理をしてデジタル処理しやすい形態に変換した上でユーザ認証票7に送付する。

【0076】ユーザ認証票7は入力された情報データを一旦RAM76に記憶し、CPU75でこの情報データとEEPROM79に記録されている正当ユーザの生物学的情報データを読み出しながら両者を突き合わせて比較する。その結果、両者が許容範囲内で類似していてサービスを利用しようとする人間がユーザ認証票7の正当な所有者ということが認証できれば認証利用所4に合格を通知し、この認証にパスしなければ拒絶を通知する。

【0077】認証利用所4は、ユーザ認証票7のユーザ認証結果に満足すれば利用者8に所望のサービスを提供する。また、さらに慎重なユーザ認証を必要とする場合は末端認証局3や中間認証局2に照会を行って、その結果と合わせて判定する。なお、認証利用所4が末端認証局3を兼ねていても良いことは言うまでもない。各所に生物学的情報データを配布する割合は任意であるが、第1実施例で例示したと同様に下位水準の認証に用いるものほど大きな割合にすると通信における負担が軽くなりシステムの運用上有利で、ユーザ認証票7における割合を60%以上にすることが好ましい。

【0078】本実施例では、高性能ICカードからなるユーザ認証票7を活用することによりユーザ認証装置41の演算上の負担を軽減し装置のコストを低減できることから、認証利用所4の機能を調えるのに必要とされる費用が小さくなるので、システムに参加するための障壁が低くなりより利用しやすくなることができる。また、ユーザ認証票内で情報処理を完結させるので、認証票のメモリに外部からアクセスできない読み出し不可領域を設けて、ここに認証データなど重要な情報を記録して漏洩を防ぐようにして安全性をより向上させることができる。

【0079】

【発明の効果】以上詳細に説明した通り、本発明のユー

18

ザ認証システムを用いれば、認証利用所において直接にユーザが入力する入証情報と認証票内の生物学的特徴データを照合し、より高度の保証を欲するときに上位の認証局に入証情報の一部を伝送してユーザ認証をするため、情報処理の大部分を認証利用所で行って通信回路に大きな負荷をかけることなく、安全性の要求水準に対応したユーザ認証を得ることができる。また、入証情報を分割することにより侵襲に対して極めて強いユーザ認証システムの構築が可能となる。

【図面の簡単な説明】

【図1】本発明の実施例のユーザ認証システムを示すブロック図である。

【図2】本実施例に用いられるユーザ認証装置の例を示す斜視図である。

【図3】本実施例におけるユーザ認証装置の回路ブロック図である。

【図4】本実施例に使用するユーザ認証票の構成例を示すブロック図である。

【図5】本実施例におけるユーザ認証票を発行する手順例を示す流れ図である。

【図6】本実施例における利用所における認証の手順例を示す流れ図である。

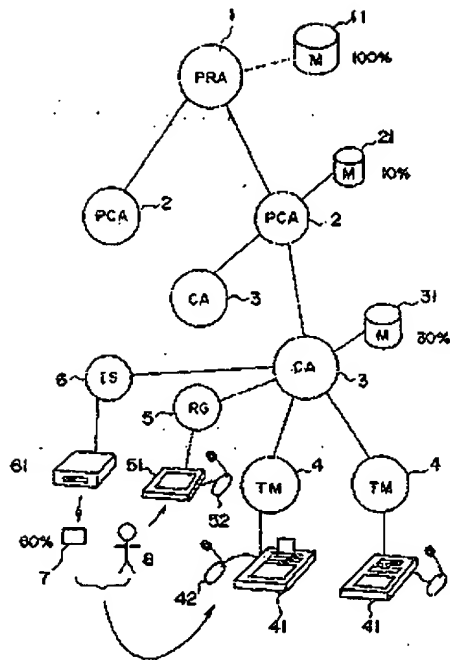
【符号の説明】

- 1 認定登録局
- 11 切離し可能な記憶装置
- 2 中間認証局
- 21 記憶装置
- 3 末端認証局
- 31 記憶装置
- 4 認証利用所
- 41 ユーザ認証装置
- 5 ユーザ登録所
- 51 入証入力装置
- 52 マイクロホン
- 6 認証票発行所
- 61 認証票発行装置
- 7 ユーザ認証票
- 71 接続端子
- 73 非接触電極
- 8 ユーザ

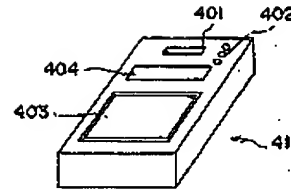
(11)

特開平11-338826

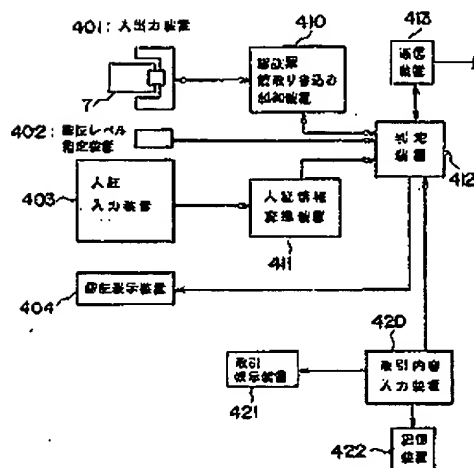
【図1】



【図2】



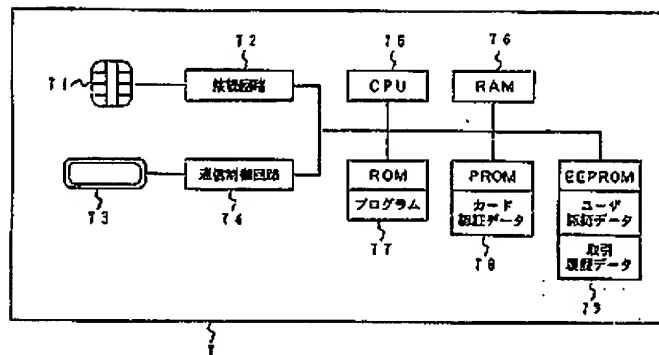
【図3】



(12)

特開平11-338826

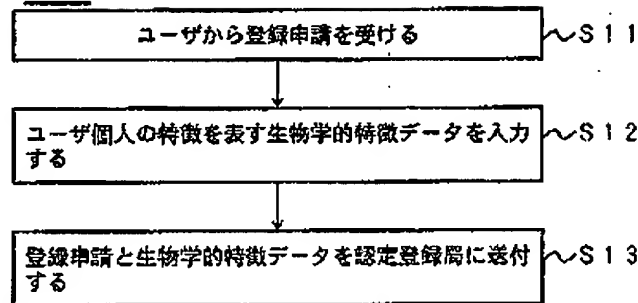
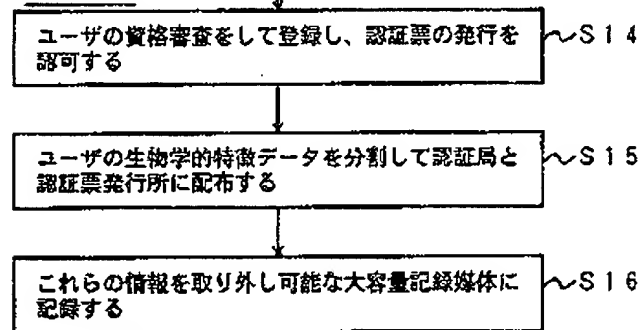
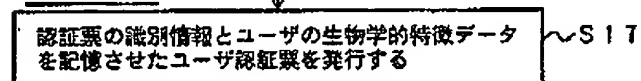
【図4】



(13)

特開平11-338826

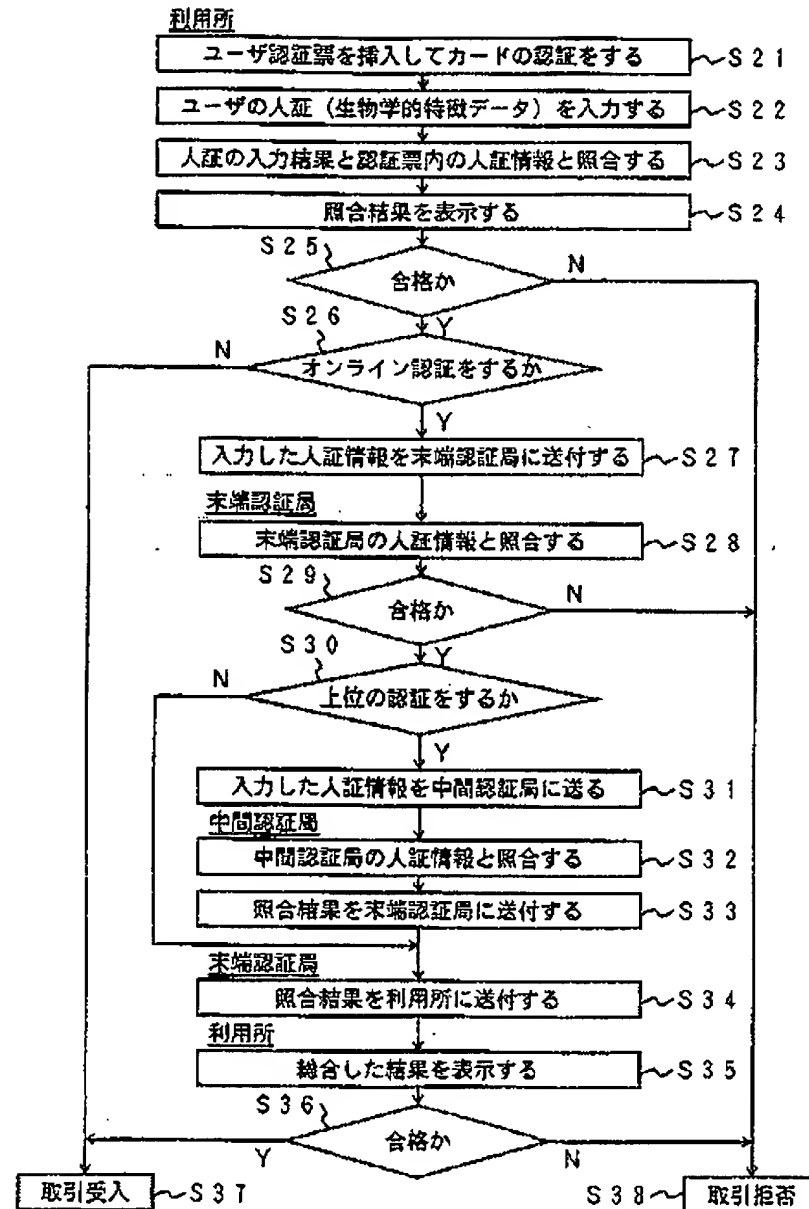
【図5】

ユーザ認証票の発行登録所認定登録局認証票発行所

(14)

特開平11-338826

【図6】

利用所における認証

(15)

特開平11-338826

【手続修正書】
 【提出日】平成11年4月19日
 【手続修正1】
 【補正対象書類名】明細書
 【補正対象項目名】発明の名称
 【補正方法】変更
 【補正内容】
 【発明の名称】 ユーザ認証システムとユーザ認証装置
 【手続修正2】
 【補正対象書類名】明細書
 【補正対象項目名】特許請求の範囲
 【補正方法】変更
 【補正内容】
 【特許請求の範囲】
 【請求項1】 ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、該ユーザに対してその生物学的特徴データのうち分割された一部を記録したユーザ認証票を発行する認証票発行所と、該ユーザ認証票の情報を読み取る認証票読取り装置とユーザの生物学的特徴データを入力する人証取得装置を設けた認証利用所と該認証利用所と情報通信路で接続された少なくとも1個の認証局を備えてなるユーザ認証システムであって、前記登録所において取得したユーザの生物学的特徴データのうち前記ユーザ認証票に記録しない部分を該認証局に記録しておいて、該認証利用所において前記認証票読取り装置で読みとるユーザ認証票の記録内容と前記入証取得装置に入力された前記ユーザの生物学的特徴データを比較することにより該ユーザが該ユーザ認証票の正当な所有者であることを認証すると共に、さらに高度な認証を行うときには前記認証局が前記認証利用所からの照会に応じて前記ユーザ認証票において欠けている生物学的特徴データの部分を比較して認証した結果を前記認証利用所に送付することを特徴とするユーザ認証システム。
 【請求項2】 前記認証利用所における認証のための演算を前記ユーザ認証票の演算機能を用いて行うことを特徴とする請求項1記載のユーザ認証システム。
 【請求項3】 前記情報通信路に流す情報は暗号化することを特徴とする請求項1または2記載のユーザ認証システム。
 【請求項4】 前記2個以上の認証局が、前記登録所において取得したユーザの生物学的特徴データのうち前記ユーザ認証票に記録しない部分を分割して記録しておいて、各認証局毎に前記認証利用所もしくは他の認証局からの照会に応じて自己の記憶する生物学的特徴データの部分を比較して認証するようにしたことを特徴とする請求項1から3のいずれかに記載のユーザ認証システム。
 【請求項5】 前記ユーザ認証システムが前記登録所において取得したユーザの生物学的特徴データを記録する

記憶装置を設けた認証局を備えることを特徴とする請求項1ないし4のいずれかに記載のユーザ認証システム。
 【請求項6】 前記認証局における生物学的特徴データを記録した記憶媒体が該ユーザ認証システムの情報通信路から切り離せることを特徴とする請求項5記載のユーザ認証システム。
 【請求項7】 前記生物学的特徴データが登録動作に伴う動的情報を加味した登録であることを特徴とする請求項1から6のいずれかに記載のユーザ認証システム。
 【請求項8】 前記生物学的特徴データとして複数のものを登録して、入力されたデータにより異なる取引を行うことを特徴とする請求項1から7のいずれかに記載のユーザ認証システム。
 【請求項9】 ユーザ認証票に記録された情報を読み取る認証票読取り装置と、ユーザの生物学的特徴データを入力する人証取得装置と、前記認証票読取り装置で読み取ったユーザ認証票に記録されている生物学的特徴データと前記入証取得装置に入力された前記ユーザの生物学的特徴データを比較して合否を判定する判定装置と、人証取得装置に入力されたユーザの生物学的特徴データの少なくとも一部を外部の認証局に送信し認証の判定結果を受け取る通信装置と、判定結果を出力する表示装置を備えるユーザ認証装置。
 【請求項10】 前記入証取得装置が手書き図形取り込み機能を有するものであることを特徴とする請求項9記載のユーザ認証装置。
 【手続修正3】
 【補正対象書類名】明細書
 【補正対象項目名】(0008)
 【補正方法】変更
 【補正内容】
 【(0008)】
 【課題を解決するための手段】上記課題を解決するため、本発明のユーザ認証システムは、ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する認証票発行所と、ユーザ認証票の情報を読み取る認証票読取り装置とユーザの生物学的特徴データを取得する人証取得装置を設けた認証利用所と、認証利用所と情報通信路で接続された少なくとも1個の認証局を備え、登録所において取得したユーザの生物学的特徴データのうちユーザ認証票に記録しない部分を認証局に記録しておいて、認証利用所の認証票読取り装置で読みとったユーザ認証票の記録内容と人証取得装置で取得したユーザの生物学的特徴データを比較することによりユーザ認証すると共に、さらに高度な認証が必要ときに認証局で認証利用所からの照会に応じてユーザ認証票において欠けている生物学的特徴データの部分を比較して認証した結果

(15)

特開平11-338826

を認証利用所に送付して認証を行うことを特徴とする。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正内容】

【0009】なお、本明細書では、人の意志により制御しきれないため他人と区別できるような個体に固有の特徴を生物学的特徴という。このような生物学的特徴には、指紋や掌紋、虹彩や網膜のパターン、DNA情報など生来のもののみならず、筆跡、声紋など習慣などにより形成されるものもあり、今後より確実で容易に認識できる生物学的特徴が見出される可能性がある。また、本発明のユーザ認証システムは、ユーザ認証票の演算装置を用いて、記録されている生物学的特徴データの内容と人証取得装置で取得されたユーザの生物学的特徴データを比較し、またさらに認証局の認証結果を統合することによりユーザ認証票の正当な所有音であることを認証することを特徴とする。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正内容】

【0010】なお、情報通信路を介して相互に交換する情報は暗号化して安全性を保證することが好ましい。

【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正内容】

【0011】また、2個以上の認証局があって、登録所で取得したユーザの生物学的特徴データのうちユーザ認証票に記録しない部分を分割して記録しておいて、各認証局毎に認証利用所もしくは他の認証局からの照会に応じて自己の記憶する生物学的特徴データの部分を比較して認証するようにすることがより好ましい。さらに、ユーザ認証システムには登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認証局を備えてもよい。また、認証局における生物学的特徴データを記録した記憶媒体はユーザ認証システムの情報通信路から切り離せるようになっていたことが好ましい。なお、生物学的特徴データとして入力過程を加味した筆跡を用いてもよい。

【手続補正7】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】変更

【補正内容】

【0015】さらに、認証利用所と情報通信路で接続さ

れた認証局にユーザの生物学的特徴データのうちユーザ認証票に記録しない残りの部分を記録しておいて、認証利用所からの照会に応じて生物学的特徴データの部分を比較して認証するようにする場合は、必要情報を分割して記憶しておくので、例えば認証票に記録されたデータから生物学的特徴データを復元しても認証システムを突破することはできないし、認証票から認証に用いるデータを複製することもできない。また、たとえ認証票の記憶内容を改竄しても認証局における情報が保全されているため他人のなりすましを排除することができる。なお、本発明の方法は分割されたデータを1箇所に集めて再統合して判定する従来の分割方式と異なり、認証利用所と認証局がそれぞれ手元の生物学的特徴データに基づいて認証を行った結果を利用するものであって、元のデータ全体が再現されることがないので、データの秘匿が保持され安全性が極めて高い。あるいはまた、認証局がアタックされた場合にもユーザの所有するユーザ認証票の情報まで改竄することができないため安全である。なお、情報通信路に流す情報が暗号化されたものであれば、通信路の途中で情報を窃取する者があっても解読しにくい為安全性が向上する。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0021

【補正方法】変更

【補正内容】

【0021】本発明のユーザ認証システムで使用する生物学的特徴データとして入力過程を加味した筆跡を用いてもよい。筆跡は個人の生物学的特徴をよく表して他人のなりすましが難しく、かつ入力する装置および解析する装置が比較的容易に得られるという利点がある。ユーザを識別するために書いて貰う文字や図形は適当なものでよいが、自己の氏名を表すサインなどは再現性がよいので好ましいのはいうまでもない。書き上がった筆跡は他人が真似ることができるが、書き順や筆勢など入力過程を加味することにより個体の生物学的特徴が現れるため他人には真似できなくなる。そこで、オンライン入力装置を用いて入力中の情報を加味して判定することにより信頼性の高い認証が可能になる。また、利用可能な生物学的特徴データには、この他、指紋や掌紋、声紋、虹彩や網膜のパターン、DNA情報などがある。今後より確実で容易に認識できる生物学的特徴が見出される可能性がある。

【手続補正9】

【補正対象書類名】図面

【補正対象項目名】図3

【補正方法】変更

【補正内容】

【図3】

(17)

特開平11-338826

